SIEMENS

Gigaset SX541 WLAN dsl

Gigaset

Contents

Safety Precautions 5

The Gigaset SX541 WLAN dsl 6

Local Networks with Gigaset Products 7
- Wired Local Network (Ethernet) 8
- Wireless Local Network (WLAN) 9
- Linking a Wireless Network (WLAN) to an Ethernet (LAN) 11

Internet Telephony and Connecting Analogue Telephones 12
Features and Applications 13
Procedure for Installation and Configuration 15

First Steps 16

System Requirements 16
Operating Displays and Connections 17
- Front Panel 17
- Back Panel 18

Setting up the Gigaset SX541 WLAN dsl 19
Connecting the Gigaset SX541 WLAN dsl 20

Configuring the Local Network 21

Network Configuration with Windows XP 21
- Configuring the Network 22
- Selecting a Computer Name and Workgroup 24
- Checking the Network Settings and Completing the Installation Procedure 24
- TCP/IP Settings 25
- Deactivating the HTTP Proxy 28
- Configuring a Popup Blocker 28
- Synchronising TCP/IP Settings with the Gigaset SX541 WLAN dsl 29

Network Configuration with Windows 2000 30
- Installing Network Services 30
- Selecting a Computer Name and Workgroup 31
- Installing the TCP/IP Protocol 32
- TCP/IP Settings 34
- Deactivating the HTTP Proxy 36
- Synchronising the TCP/IP Settings with the Gigaset SX541 WLAN dsl 37

Network Configuration with Windows 98 SE, ME 38
- Setting up a PC as a Client for Microsoft Networks 38
- Selecting a Computer Name and Workgroup 39
- Installing the TCP/IP Protocol 40
- Making TCP/IP Settings 41
- Deactivating the HTTP Proxy 45
- Synchronising the TCP/IP Settings with the Gigaset SX541 WLAN dsl 46

Checking the Connection to the Gigaset SX541 WLAN dsl 47

The User Interface 48

Launching the User Interface 48
The Start Screen 49
Selecting a Language 51
Elements on the User Interface 52

Basic Setup Wizard 53

Regional Options 54
Configuring Internet Connections 55
Telephony 57
Summary 58

Security Settings 59

Assigning a Password 60
SSID 61
Setting Security Functions for the Wireless Network 62
    WPA2 / WPA with Pre-Shared Key (PSK) 63
    WEP Encryption 64
Access Control Within the Wireless Network 66
Saving Settings 67

Configuring the Advanced Settings 68

Internet 69
    Internet Selection 69
    Internet Connection 70
    DNS Server 74
    MAC Address 75
    Traffic Control 76
Firewall 78
    Attack Detection 78
    Setting up Access Control to the Internet 81
Setting up the NAT Function 85
    Port Triggering 87
    Port Forwarding 88
    Opening the Firewall for Selected PCs (Exposed Host) 89
    Dynamic DNS 90
    QoS (Quality of Service) 92
LAN Configuration 93
    Assigning Static IP Addresses to Individual PCs 94
Configuring Wireless Connections 95
    Setting Wireless Security 97
    WPA2-PSK and WPA2-PSK / WPA-PSK 98
    WEP Encryption 100
    Allowed Clients 102
    Repeater Function (WDS) 103

Setting up Internet telephony (VoIP) 104
VoiP Settings 105
Extensions 107
Dialing Plans 108
Quick dial 110
USB 111
File Server 112
Web Server 115
Print Server 117

Administration and Status Information 118

Connecting to the Internet Manually 118
Regional Options 119
Internet Time 120
System Password 120
Setting up Remote Management 121
Saving and Restoring a Configuration 123
Saving Configuration Data 123
Restoring the Back-up 124
Resetting to the Factory Settings 124
Reboot 124
Updating Firmware 125
System Log 126

Status Information 127

Overview 127
Security 129
Internet 131
Traffic Control 133
Local Network 134
Wireless Network 135
Telephony 136
Device 137

Installing the Printer Port for Network Printers . 139

Introduction 139
Installing a Standard TCP/IP Printer Port Under Windows XP/2000 140
Installing a Printer on the TCP/IP Port Retrospectively 146
Installing a Printer Driver Under Windows 98 SE or ME 147
Instructions for Setting up a Printer on the PC 148

Appendix 149

Troubleshooting 149
Specifications 152
Open Source Software used in the product 154
Open Source Software Licenses 155

Glossary **167**
Index **179**

Safety Precautions

- Only use the mains adapter (12V 1A DC) that is supplied with the Gigaset SX541 WLAN dsl. Comply with the connection values and ratings when connecting the device to the mains power supply.
- Protect the device from damp.
- Never open the device. For reasons of electrical safety it may only be opened by authorised service technicians.
- The device may affect medical equipment.

Trademarks

Microsoft, Windows 98 SE, Windows ME, Windows 2000, Windows XP and Internet Explorer are registered trademarks of the Microsoft Corporation.

Mozilla Firefox is a registered trademark of the Mozilla Organization.

The Gigaset SX541 WLAN dsl

Your Siemens Gigaset SX541 WLAN dsl is a powerful but easily operated device for connecting your PC (WLAN) or your local network (LAN) to the Internet (via DSL) without the need for wires. It contains an integrated DSL modem for easily connecting the devices to the Internet.

Additionally, the Gigaset SX541 WLAN dsl provides the functions of a telephone system for Internet telephony (***VoIP***) and conventional telephony to which you can connect up to two conventional analogue terminals. You can phone via the Internet or also use an existing analogue telephone subscriber line.

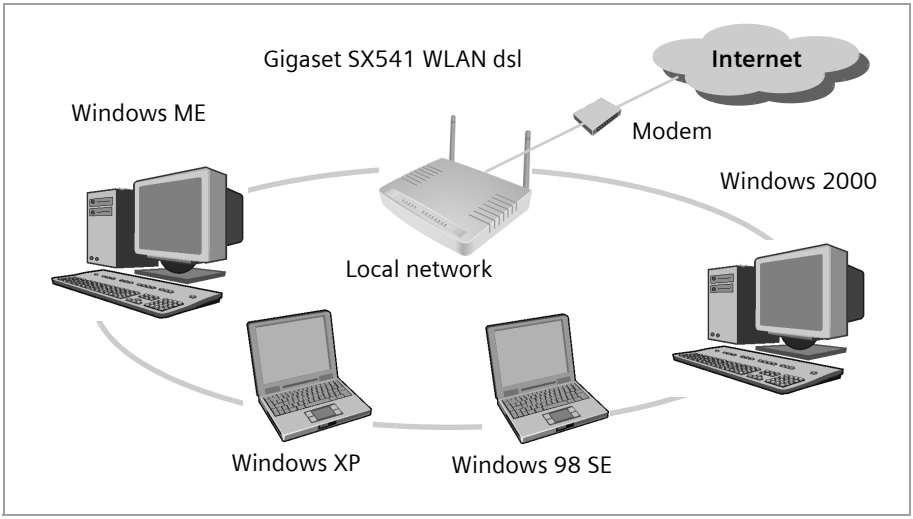
The Gigaset SX541 WLAN dsl allows several users to access the Internet simultaneously. A single user account can be shared if your Internet Provider permits this. If you want to surf the Internet or phone via the Internet at the lowest possible cost, then the Gigaset SX541 WLAN dsl is a convenient and effective solution.

You can connect your PC wirelessly to the Gigaset SX541 WLAN dsl and create a wireless local network (WLAN). For network security, wireless transmission can be encrypted using the WPA standard or 64/128-bit WEP.

Despite its extensive range of functions, the Gigaset SX541 WLAN dsl is simple to handle. It can be configured and operational within a few minutes.

Local Networks with Gigaset Products

You can use the Siemens Gigaset SX541 WLAN dsl to set up a local network, for example a home network. All the PCs in this network can communicate with each other and have access to the Internet.



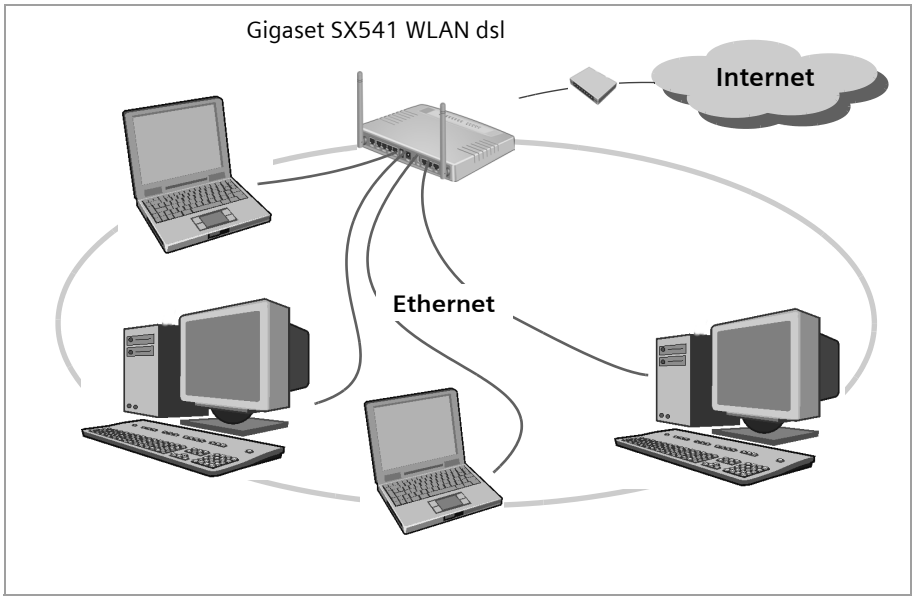
There are various ways in which you can set up the network with a Gigaset SX541 WLAN dsl. You can

- set up a wired local network (Ethernet) and allow the connected PCs access to the Internet (see page 8).
- set up a wireless local network (WLAN) and allow the connected PCs access to the Internet (see page 9).
- set up a local network comprising wireless and wired network components (see page 11).

Wired Local Network (Ethernet)

In a wired local network, PCs communicate with one another via an Ethernet cable. When the Siemens Gigaset SX541 WLAN dsl is used, it establishes the connection between the PCs. For this it has four Ethernet LAN ports for connecting four PCs. The PCs have to be equipped with a network socket (Ethernet). New PCs frequently already have this socket. For older PCs you need to install an Ethernet network card. The PC and the Ethernet LAN socket on the Gigaset SX541 WLAN dsl are connected using an Ethernet cable (CAT5). One is supplied. You can obtain additional Ethernet cables from your retailer.

The Gigaset SX541 WLAN dsl allows all PCs to access the Internet simultaneously.



Wireless Local Network (WLAN)

In a wireless local network (WLAN), PCs are linked without wires. The PCs have to be equipped with a wireless network adapter (WLAN adapter) for this purpose, such as a Gigaset PC Card or a USB Adapter.

We generally differentiate between two types of wireless network.

- Infrastructure mode
- Ad-hoc mode

Infrastructure mode

Infrastructure mode connects wireless and wired networks with one another. In addition to the mobile stations, infrastructure mode needs an access point such as the Gigaset SX541 WLAN dsl. The stations in the network always communicate via this access point in infrastructure mode. Each station that wants to be part of the wireless network must first register with the access point before it can exchange data.

The access point establishes the connection between the mobile stations of a wireless network and a wired LAN (Ethernet) or the Internet. In this case, this is described as the device's router functionality. The router sends data packets that are not addressed to stations within the network "outside" and forwards data packets originating from "outside" to the appropriate station within the network.

You can use the Gigaset SX541 WLAN dsl to connect

- wirelessly networked PCs to the Internet and
- wirelessly networked PCs to an Ethernet network.

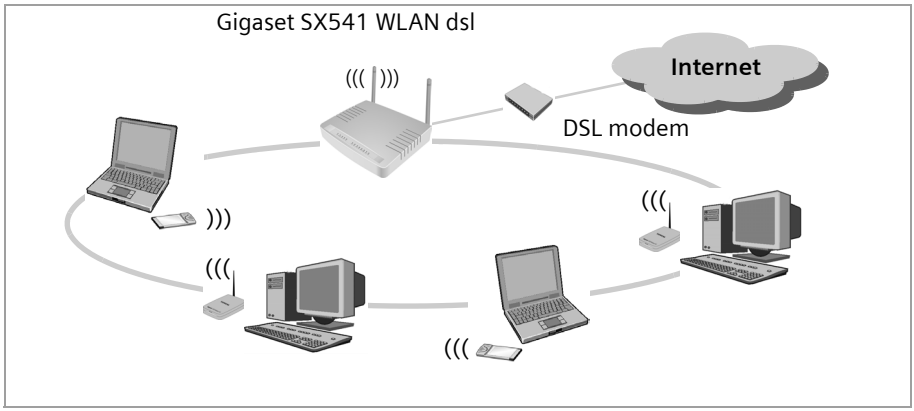
Infrastructure mode is the default configuration of the Gigaset SX541 WLAN dsl. This configuration is described in the quick guide enclosed with the router.

Ad-hoc mode

An ad-hoc network is a wireless network set up without an access point or router. The mobile network components that communicate with each other directly and without wire connections form the network "ad-hoc", i.e. as and when required. All the stations in the network have the same rights. Ad-hoc networks are used wherever communications networks have to be set up quickly and without any existing network infrastructure and where the participants are on the move.

Linking wireless networks with the Internet

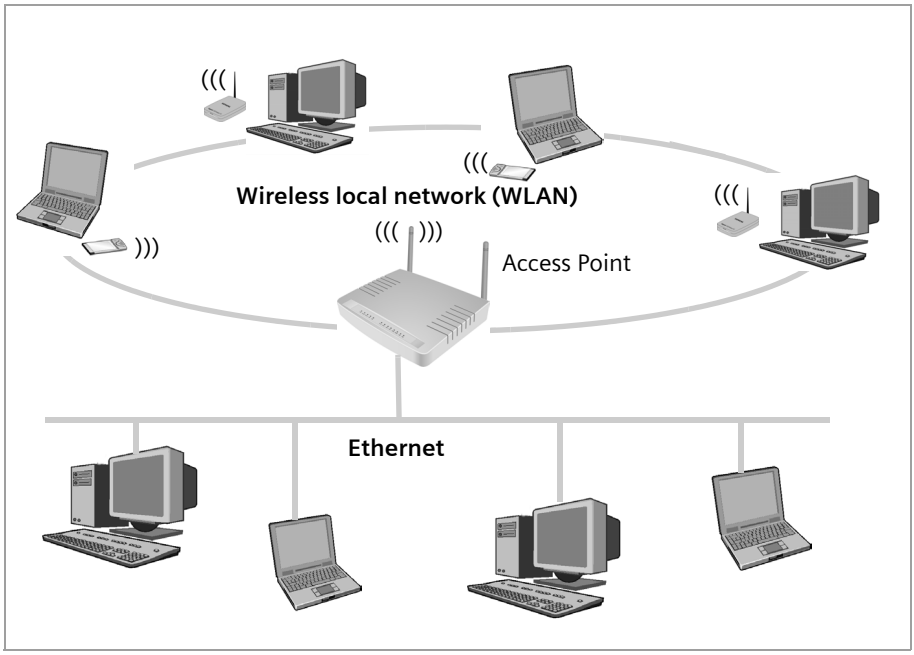
The Gigaset SX541 WLAN dsl has an ADSL interface that permits all stations within its local network to access the Internet simultaneously. To be able to use this functionality, you need a DSL or cable connection obtainable from an Internet provider. Find out whether your Internet Service Provider supports parallel access by several PCs.



This illustration shows the most common method of application. One or more PCs communicate wirelessly with the Gigaset SX541 WLAN dsl in infrastructure mode. The Gigaset SX541 WLAN dsl forwards the data to the Internet via a DSL or cable modem. Data from the Internet flows back to the PC along the same route.

Linking a Wireless Network (WLAN) to an Ethernet (LAN)

Wireless networks can work easily together with existing Ethernet networks. If you wish to connect mobile stations to an existing wired network, you must group together all mobile stations into a wireless network in infrastructure mode.



The Gigaset SX541 WLAN dsl has four Ethernet interfaces (LAN ports). Up to four PCs can be connected directly to these LAN ports.

All PCs can access the Internet via the Gigaset SX541 WLAN dsl.

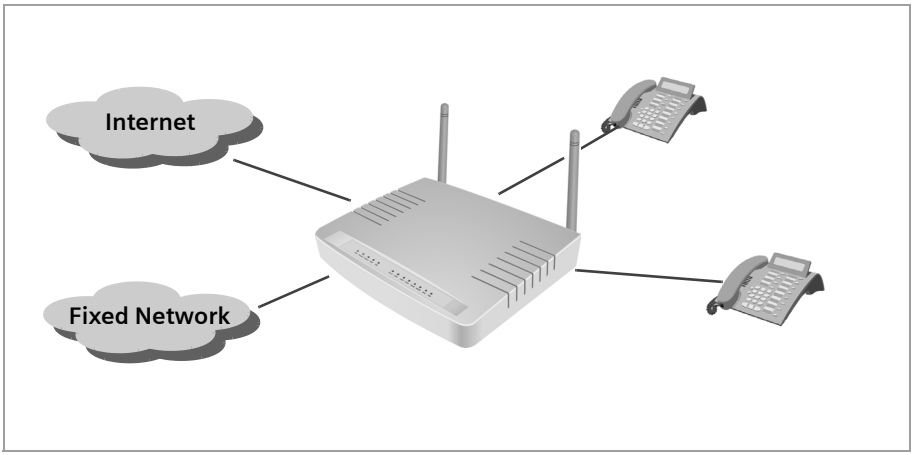
Please remember:

You can also connect an Ethernet router to a LAN port to access a larger Ethernet. If you want to link the Gigaset WLAN network to an existing network, a large number of settings have to be applied. Therefore we cannot provide a general example for this use; the configuration depends greatly on the networks in question. We recommend that such a network be configured by a specialist.

Internet Telephony and Connecting Analogue Telephones

The Gigaset SX541 WLAN dsl allows fixed network and Internet telephony (VoIP) to be combined via DSL for two analogue telephones.

With it you can optimally use the benefits of both technologies. Low priced Internet telephone rates can be availed of without the need for additional equipment. Additionally you have the possibility to use your fixed network subsequently. As a result, you can use the benefits of both technologies optimally. The particular type of telephony that is most beneficial for you will depend on your telephony behaviour and on the particular rate offered by your service provider. The Gigaset SX541 WLAN dsl gives you free choice at any time.



You can connect two arbitrary analogue telephones or base stations for cordless telephones to the telephone connections of your Gigaset SX541 WLAN dsl.

Please note that the Gigaset SX541 WLAN dsl is not intended to be directly connected to ISDN. Connection is possible via an intermediate a/b converter or an ISDN telecommunications system (e. g. Gigaset SX353isdn).

To configure the Internet telephony you need the appropriate access data for your service provider.

You can of course operate Internet telephony later on via a PC connected to the Gigaset SX541 WLAN dsl. In this case, the PC must be equipped with loudspeakers and microphone or headset and a full duplex sound card and must have the necessary software installed.

Please note that telephone access via the Internet is only possible if an Internet connection is established.

Features and Applications

The Gigaset SX541 WLAN dsl's wide range of features makes it ideal for a large number of applications, such as:

- **Internet access**

  The Gigaset SX541 WLAN dsl gives several users access to the Internet.

  – As with many DSL providers, the Internet is accessed via the PPPoE protocol. The Gigaset SX541 WLAN dsl contains an integrated PPPoE Client, which means you no longer need to set up this service on your PC yourself.

  – Shared Internet access

    If your Internet provider permits this, the Gigaset SX541 WLAN dsl supports Internet access for up to 252 users. In practice, multiple users in your network can surf the Internet simultaneously using just one Internet account.

- **Setting up a local network**

  The Gigaset SX541 WLAN dsl permits connections

  – for four devices via Ethernet ports with a transmission speed of 10 or 100 Mbps (with automatic recognition).

  – for up to 252 mobile terminals via a radio interface with a transmission speed of up to 54 Mbps. It complies with Standard IEEE 802.11g and can work with all products that satisfy Standard IEEE 802.11 b or 802.11g.

  Using a Gigaset SX541 WLAN dsl makes it easy to set up a network at home or in small offices. For example, users can exchange data or share resources on the network, such as a file server or printer. You can connect a USB hard disk, a USB stick or a printer to the USB interface of the Gigaset SX541 WLAN dsl and make them available to all users in your network.

  The Gigaset SX541 WLAN dsl supports DHCP for the dynamic IP configuration of the local network and DNS for domain name mappings.

- **Connecting analogue telephones and Internet telephony**

  The Gigaset SX541 WLAN dsl allows

  – Internet telephony via the DSL connection

  – Fixed network telephony via the analogue connection

  – connecting two analogue telephones for Internet telephony and for fixed network conversation

  Data transmission for VoIP is performed by means of SIP with high connection and voice quality. Should it happen that the Internet connection fails, you can telephone via the fixed network.

- **Security functions**

  The Gigaset SX541 WLAN dsl offers comprehensive security measures:

  – Firewall protection against unauthorised access from the Internet

    All the PCs in the local network use the Gigaset SX541 WLAN dsl's Public IP address for their Internet connections, which makes them 'invisible' on the Internet. The Gigaset SX541 WLAN dsl only allows access from the Internet if it has been requested from the local network.

    With the firewall the Gigaset SX541 WLAN dsl also offers comprehensive protection against hacker attacks.

  – Service filtering and URL filtering

    The Gigaset SX541 WLAN dsl can filter Internet access. This allows you to determine which PCs may access which Internet services.

    In addition, you can deactivate access to certain Internet domains and sites (URL filtering).

  – Access control and encryption for the local network

    You can use various encryption methods and authentication methods (WEP, WPA/WPA2-PSK,WPA/WPA2, MAC access control) to prevent unauthorised access to your wireless LAN or to make data illegible to unauthorised parties.

- **Offering your own services on the Internet**

  – If you want to offer your own services on the Internet, you can configure the Gigaset SX541 WLAN dsl as a virtual server without permitting further access to the local network.

  – Exposed Host

    You can set up a PC in your local network to be a virtual server and release it for unrestricted access from the Internet.

Procedure for Installation and Configuration

1. First install an Ethernet network card or a wireless Network adapter such as a Gigaset PC Card or a Gigaset USB Adapter in the PCs you want to connect to the Gigaset SX541 WLAN dsl. The installation is described in the user guides for the products.

   Please remember:
   When installing wireless network adapters, use the default SSID for the Gigaset SX541 WLAN dsl: **ConnectionPoint**.

2. Then make the necessary connections (PCs, telephones, splitter) to the Gigaset SX541 WLAN dsl and switch on the device on (see Section "Connecting the Gigaset SX541 WLAN dsl" on page 20).
3. Before the PCs can communicate with the Gigaset SX541 WLAN dsl and with each other in a local network, you have to change their network settings. Configure these network settings on **one** PC first so that it can establish a connection to the Gigaset SX541 WLAN dsl. You can then use this PC to configure the device. To find out how to do this, refer to "Configuring the Local Network" on page 21.
4. With a wireless connection you establish the link from the PC's wireless network adapter to the Gigaset SX541 WLAN dsl. This is described in the user guide for the network adapter.
5. Then configure the Gigaset SX541 WLAN dsl to activate the device's Internet access (refer to the section "Basic Setup Wizard" on page 53). Access data is required from your Internet service provider for this purpose.

- If you want to connect more PCs to the Gigaset SX541 WLAN dsl, configure their network settings to set up the local network (refer to the section entitled "Configuring the Local Network" on page 21).
- If you want to operate Internet telephony via the Gigaset SX541 WLAN dsl, you have to configure the access data for your VoIP provider (see page 105).
- If you want to use the Gigaset SX541 WLAN dsl's other functions, for example the comprehensive security features, use the router's Security Setup (see page 59) or the Advanced Settings menu (see page 68).

First Steps

System Requirements

To operate your Gigaset SX541 WLAN dsl you need:

- A PC with
  - an 802.11g or 802.11b-compatible wireless Network adapter

    Note:
    The maximum data transfer rate for 802.11b-compatible network adapters is 11 Mbps and for 802.11g-compatible network adapters is 54 Mbps.

  or

  - an Ethernet device
- A Web browser, such as Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.0, for configuring your Gigaset SX541 WLAN dsl
- For Internet access
  - a DSL connection,
  - the access data for your Internet Provider.
- For operating telephones:
  - an analogue phone,
  - an analogue phone line if you want to use fixed network telephony,
  - the access data for your VoIP provider if you want to use Internet telephony.

Operating Displays and Connections

Front Panel

LED displays

The front panel of the device contains LED displays that show the operating state and simplify installation and fault finding in the network.

The LEDs show the following (from right to left):

LED	State	Status
PWR	On	The Gigaset SX541 WLAN dsl is powered on.
	Off	The Gigaset SX541 WLAN dsl is powered off.
ADSL	On	The DSL line is connected and the ADSL port is operational.
	Flashing slowly	The DSL line is being synchronised.
	Flashing quickly	The DSL line synchronisation is in its last phase.
	Off	The DSL line is not connected or the interface is not synchronised.
Online	On	Connection to the Internet has been established.
	Off	There is no Internet connection.

LED	State	Status
WLAN	On	The radio interface is active.
	Flashing	The Gigaset SX541 WLAN dsl is sending or receiving data on the radio interface.
	Off	The radio interface has been deactivated or no radio signal is being received.
LAN1 – LAN4	On	A device is connected to the relevant LAN port.
	Flashing	The LAN port is sending or receiving data (traffic).
	Off	There is no device connected.
USB	On	A device is connected to the Gigaset SX541 WLAN dsl via the USB port.
	Off	There is no device connected.
VoIP	On	At least one SIP account is registered successfully.
	Flashing	The device tries to register a SIP account.
	Off	No SIP account is registered or enabled.
Phone 1/ Phone 2	On	The relevant telephone's receiver has been lifted for a call.
	Flashing	The telephone is ringing or someone is waiting on the line.
	Off	The telephone receiver has rung off. Presently, there is no call or telephone conversation.
Line	On	One of the connected telephones' receivers has been lifted for a call (fixed network).
	Flashing	The telephone is ringing and there is a fixed network call or someone is waiting on the line.
	Off	Presently, there is no fixed network connection.

Back Panel

The back panel of the Gigaset SX541 WLAN dsl houses the sockets.

Element	Description
ADSL	Socket for connecting the integrated modem with the splitter's DSL connection.
LAN1 – LAN4	Four 10/100 Mbps switch sockets with automatic recognition (RJ-45). You can connect up to four Ethernet devices (such as PCs, a Hub or Switch).
ON/OFF	Use this switch to power on or off the device.
PWR	Socket for the mains adapter supplied (12V 1A DC). **Warning**: Using the wrong power supply unit may damage the Gigaset SX541 WLAN dsl.
Reset	Reboot function: Press the button for longer than 1 second but less than 5 seconds to reboot the device. This does not affect the configuration settings. Reset function: Press the button behind the small opening on the bottom of the device for at least 5 seconds to return all settings to the factory settings. **Warning**: This will clear all the configuration settings you have made. Updated firmware will not be affected.
USB	USB port for printer or USB bulk memory.
Phone1 / 2	Sockets for connecting analogue telephones.
Line	Socket for connecting the Gigaset SX541 WLAN dsl with the splitter's telephone socket.

Setting up the Gigaset SX541 WLAN dsl

The Gigaset SX541 WLAN dsl can be set up in any suitable location in your home or office. You do not need any special wiring. However, you should comply with the following guidelines:

- Operate the Gigaset SX541 WLAN dsl only indoors within a temperature range of +5 to +40 °C. Do not position the Gigaset SX541 WLAN dsl near sources of heat. Do not cover the ventilation slots. High temperatures can damage the device.
- A mains socket for 220/240V~ and a connection socket for the splitter or LAN must be available where you set up the Gigaset SX541 WLAN dsl.
- Do not position the device in the immediate vicinity of stereo equipment, TV sets or microwave ovens. This may cause interference.
- Position the Gigaset SX541 WLAN dsl so that it is as near to the centre of your wireless network as possible. Make sure that where you position the Gigaset SX541 WLAN dsl provides optimum reception throughout the house or office. You can improve the reception quality by aligning the antenna (turn and/or tilt).
- Position the Gigaset SX541 WLAN dsl on a non-slip surface. The router feet do not normally leave any traces on the surface they are on. However, some furniture surfaces may contain substances that attack and soften the router's rubber feet. The feet may well mark the furniture surface in this case.

- Do not place the Gigaset SX541 WLAN dsl on any furniture surface that could be affected by the heat from the device.
- Position the Gigaset SX541 WLAN dsl so that it cannot fall.
- Lay the cables so that nobody can trip over them.

Connecting the Gigaset SX541 WLAN dsl

Connect your Gigaset SX541 WLAN dsl as described in the quick start guide.

Your Gigaset SX541 WLAN dsl is ready for use:

- The **PWR** LED on the front lights up.
- the **ADSL** LED flashes to indicate that the DSL connection is being synchronised. Once this process has been concluded, the ADSL LED is permanently illuminated.
- The **WLAN** LED lights up to indicate that the Gigaset SX541 WLAN dsl is ready to open wireless connections.

  The radio link to a PC that is connected by means of a wireless network adapter is opened automatically provided the network adapter has been configured with the same SSID as the Gigaset SX541 WLAN dsl. It can take a few seconds for the wireless connection to be established. The **WLAN** LED flashes when data is sent or received via this connection.
- The **LAN** LEDs light up if a device is connected to the corresponding LAN connection.

In order to communicate via the Gigaset SX541 WLAN dsl, the network must be configured on the connected PC. This usually takes place automatically (see page 21).

In order to gain access to the Internet via the Gigaset SX541 WLAN dsl, you must configure the device's DSL connection (see page 55).

In order to operate Internet telephony via the Gigaset SX541 WLAN dsl, you must configure the VoIP connection (see page 104).

You will find information on how to operate devices on the USB port of the Gigaset SX541 WLAN dsl on page 117 for printers and on page 112 for external bulk memories.

Configuring the Local Network

Once you have set up the hardware and connected all the devices, you have to configure the network settings of all the PCs that will communicate with each other via the Gigaset SX541 WLAN dsl.

In this chapter we assume that you will use the Gigaset SX541 WLAN dsl's DHCP service. This means that the IP addresses are automatically assigned to the PCs (Dynamic IP addresses). This is also the device's default setting.

In many cases, however, it is advisable to assign Static IP addresses, for example if you wish to run a wireless network in Ad-hoc mode. A description of how to configure the dynamic address assignment on the Gigaset SX541 WLAN dsl is given in the section "LAN Configuration" on page 93.

If your network has already been set up, you can read on from "The User Interface" on page 48.

The network configuration varies depending on the Windows operating system you are using. You will find the procedure described below for Windows 98 from page 38, for Windows XP from page 21 and for Windows 2000 from page 30.

Have your Windows Installation CD to hand. You may be prompted to insert it.

Please remember:

The Windows user interfaces depicted in this guide may differ from those on your screen because of the settings you have made. The illustrations always reflect the state after immediately installation.

Network Configuration with Windows XP

To integrate a PC with Windows XP into a network that is configured with a Gigaset SX541 WLAN dsl, you must carry out the following steps:

1. Configure the network (see below)
2. Select a computer name and workgroup (see page 24)
3. Check the network settings and complete the installation procedure (see page 24)
4. Make TCP/IP settings (see page 25)
5. Deactivate the http proxy (see page 28)
6. Configure the popup blocker (see page 28)

Note:

The name of the menu items may differ slightly from one version of Windows XP to another. However, the configuration settings described below apply generally.

Configuring the Network

Please remember:

Make sure that the ***Use Windows to configure the settings*** function is deactivated.

This can be done as follows:

➔ Click ***Start*** – ***Settings*** – ***Control Panel*** – ***Network Connections*** – ***LAN or High-Speed Internet***.
A window opens showing the properties of this connection.
In some versions of Windows XP, this window is opened by right-clicking the mouse on the Properties menu item.

➔ On the ***General*** tab, click the ***Properties*** button.
On the ***Wireless networks*** tab, deselect the option ***Use Windows to configure the settings***.

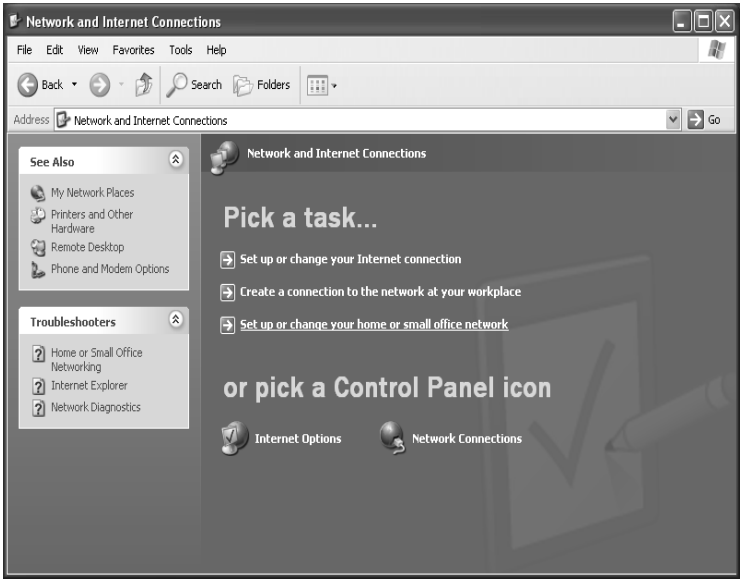
Configuring the network in this case means selecting ***Internet connection*** as the connection method. You can do this with the network wizard.

➔ Click ***Start*** – ***Settings*** – ***Control Panel***.

➔ Open the ***Network Connections*** screen (by double-clicking or by using the right mouse key).

➔ Under ***Network Tasks,*** select the option ***Set up or modify a home network or small office network***.

The network installation wizard is started.


Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
or pick a Control Panel icon
Internet Options
Network Connections

➔ Skip the welcome screen and the checklist by clicking ***Next*** twice.

You will be prompted to select a connection method.

➔ Select ***Other Method*** and confirm with ***Next***.

You will now see a screen listing various connection methods.

Network Setup Wizard
Select a connection method.
Select the statement that best describes this computer:
This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.
This computer connects to the Internet through another computer on my network or through a residential gateway.
View an example.
Other
Learn more about home or small office network configurations.
< Back
Next >
Cancel

➔ Select ***This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer*** and click ***Next***.

➔ In the next window select your network adapter and click ***Next***.

➔ Skip the message ***This network configuration is not advisable*** by clicking ***Next***.

Selecting a Computer Name and Workgroup

You now have to specify a name for the PC and assign it to a workgroup.

➔ Enter the name the PC is to appear under in the network.This name must be unique within the network. You can complete the ***Computer description*** field or leave it blank. Then click ***Next***.

➔ Enter a name for the workgroup the PC is to belong to. This name must be identical for all the PCs in the network. Then continue by clicking ***Next***.

Checking the Network Settings and Completing the Installation Procedure

You will now see a screen in which you can check the settings you have made and make any changes you want.

➔ Click ***Back*** if you want to make any changes or click ***Next*** if you want to leave them unchanged.

If you do not want to install any more PCs:

➔ Select ***Only finish the wizard as it is not run on other computers*** and confirm by clicking ***Next*** twice.

➔ Answer the question ***Do you want to restart your computer now?*** with ***Yes***.

If you want to set up a network on other PCs with Windows XP, you can now create a network installation disk.

➔ Select ***Create a network installation disk*** and click ***Next***.

➔ Follow the screen instructions and insert a disk. The necessary data will now be copied. Now label the disk as ***Network installation***.

➔ Confirm the next two screens with ***Next*** and complete the installation procedure by rebooting the PC.

After this your home network will have been installed.

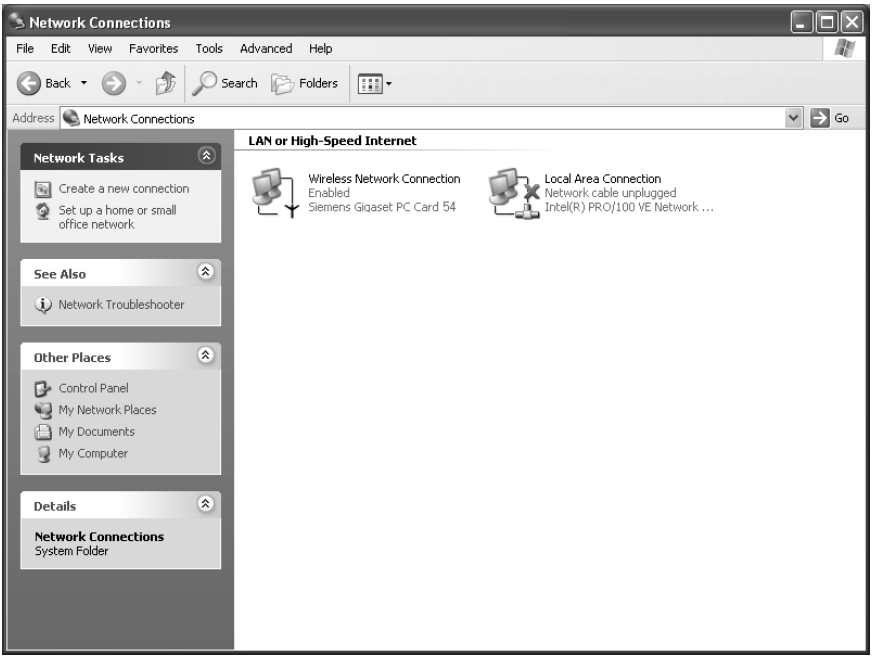
To set up the network on the other PCs with the same settings, insert the disk in the drive and run ***Netsetup*** with a double click.

TCP/IP Settings

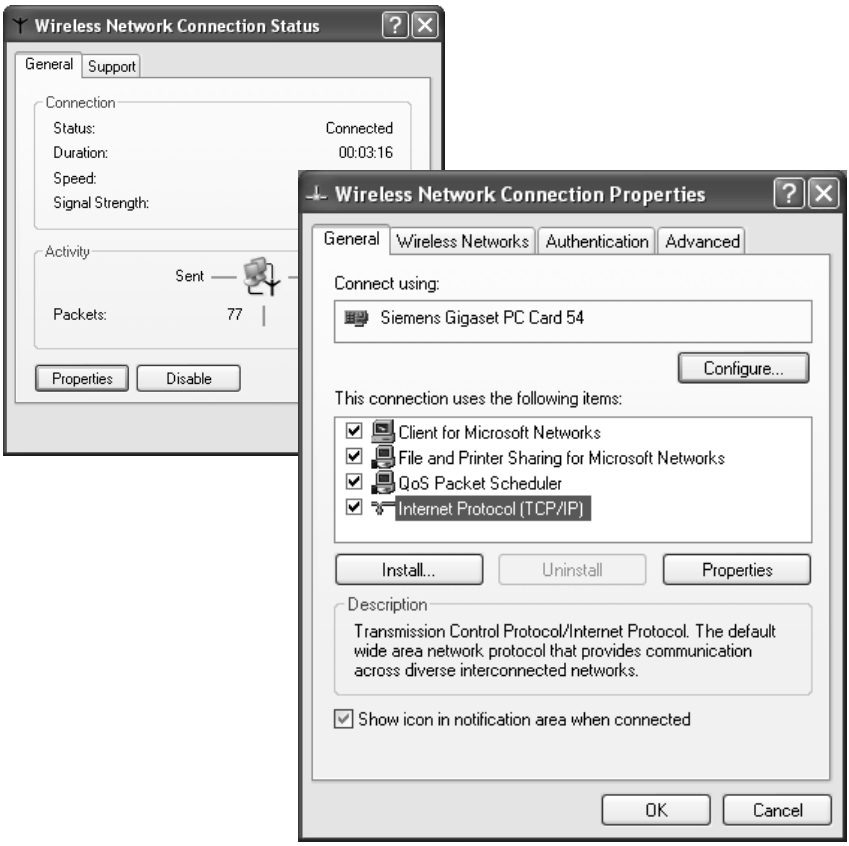
The TCP/IP Protocol requires certain settings which you should now make or check so that it can function smoothly.

➔ Click ***Start*** – ***Settings*** – ***Control Panel***.

➔ Select ***Network Connections***.

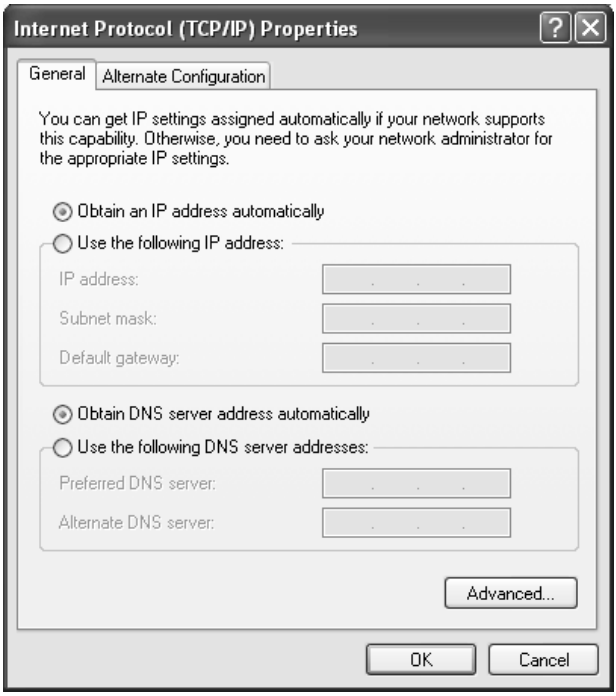


➔ Double-click the LAN connection with which you are connected to the Gigaset SX541 WLAN dsl.



➔ Click ***Properties***.

➔ Select ***Internet protocol (TCP/IP)*** and click ***Properties***.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

➔ If the ***Obtain IP address automatically*** and ***Obtain DNS server address automatically*** options have already been activated, your PC is already configured for DHCP. Click ***Cancel*** and close the following windows with ***OK*** to save your network configuration.

➔ If the ***Obtain IP address automatically*** and ***Obtain DNS server address automatically*** have not yet been activated, select them now and click ***OK***. Close the following screens.

Deactivating the HTTP Proxy

Make sure that the HTTP Proxy in your Web browser is deactivated. This function must be deactivated so that your Web browser can access your Gigaset SX541 WLAN dsl's configuration pages.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First decide which browser you are using and then follow the appropriate steps.

Internet Explorer

➔ Open Internet Explorer and click ***End***. Click ***Tools*** and then on ***Internet Options***.

➔ In the ***Internet Options*** window, click the ***Connections*** tab.

➔ Click ***Settings***.

➔ Deactivate all options in the ***Settings for Local Area Network (LAN)*** window.

➔ Click ***OK*** and then ***OK*** again to close the ***Internet Options*** window.

Mozilla Firefox

➔ Open Mozilla Firefox. Click ***Tools*** and then on ***Settings***.

➔ In the ***Settings*** window, click ***Connection Settings...*** .

➔ In the ***Connection Settings*** window, select the option ***Direct connection to the Internet***.

➔ Click ***OK*** to finish.

Configuring a Popup Blocker

If working with Windows XP Service Pack 2, popups are blocked by default. You must allow popups for the configuration program in order to start it. Carry out the following steps:

➔ Right-click the browser information bar.

➔ Select ***Allow popups from this screen***.

➔ Confirm the dialogue window by clicking on ***OK***.

The configuration screens for the Gigaset SX541 WLAN dsl are now allowed as popups.

You can make additional settings for popups within Internet Explorer

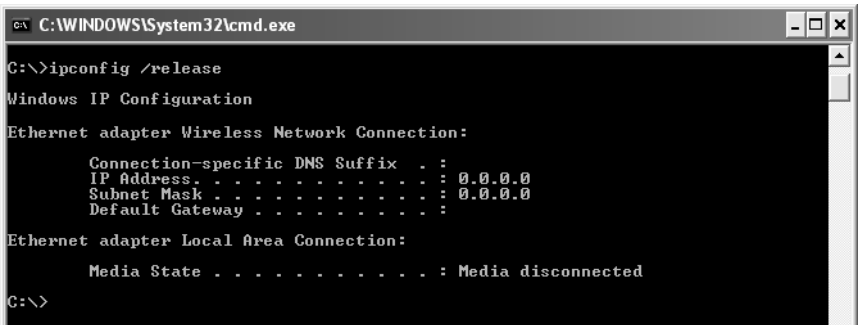
- via the ***Tools – Popup manager*** menu item or
- via ***Tools – Internet Options*** on the ***Privacy*** tab.

Synchronising TCP/IP Settings with the Gigaset SX541 WLAN dsl

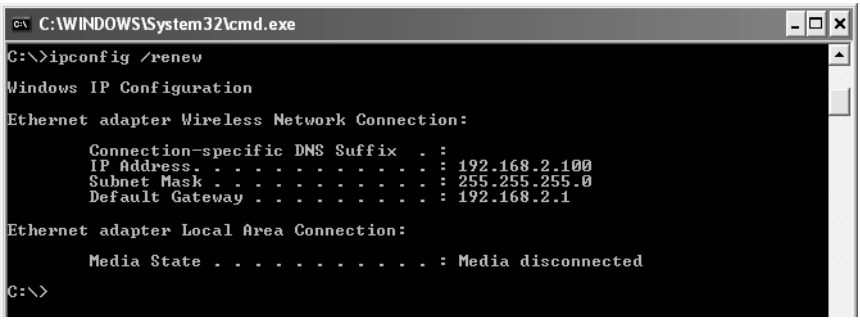
You have now configured your PC so that it is ready to be connected to the Gigaset SX541 WLAN dsl. You now have to release the old TCP/IP settings and synchronise them with the settings of your Gigaset SX541 WLAN dsl.

➔ Click ***Start*** on the Windows Desktop and then ***Programs***, followed by ***Accessories*** and finally ***Command prompt***.

➔ In the ***Command prompt*** window, enter the **`ipconfig /release`** command and press the ENTER key.


C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /release
Windows IP Configuration
Ethernet adapter Wireless Network Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
Ethernet adapter Local Area Connection:
Media State . . . . . : Media disconnected
C:\>

➔ Then enter the **`ipconfig /renew`** command and press the ENTER key.


C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /renew
Windows IP Configuration
Ethernet adapter Wireless Network Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
Ethernet adapter Local Area Connection:
Media State . . . . . : Media disconnected
C:\>

If the default IP address (192.168.2.1) of the Gigaset SX541 WLAN dsl was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 255). The ***Subnet Mask*** must always be 255.255.255.0 and the ***Standard Gateway*** must have the IP address of the Gigaset SX541 WLAN dsl (192.168.2.1). These values confirm that your Gigaset SX541 WLAN dsl is working.

➔ Enter **`exit`** and press the Enter key to close the ***Command prompt*** window.

Network Configuration with Windows 2000

To integrate a PC with Windows 2000 into a network that is configured with a Gigaset SX541 WLAN dsl, you must carry out the following steps:

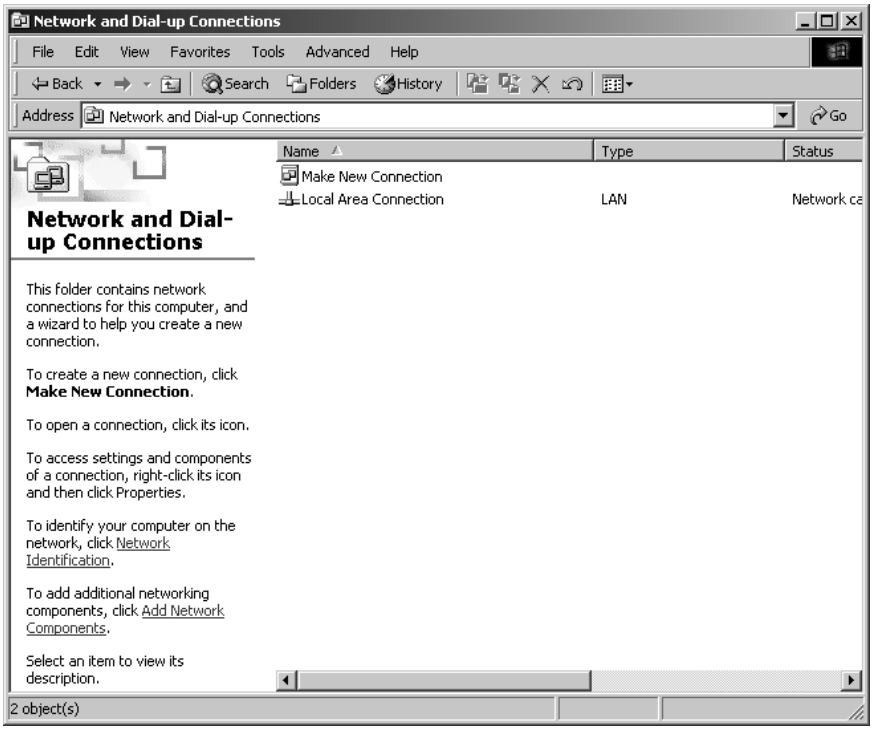
1. Install the network services (see below).
2. Select computer names and workgroup (see page 31).
3. Install the TCP/IP protocol (see page 32).
4. Make TCP/IP protocol settings (see page 34).
5. Deactivate the http proxy (see page 36).
6. Synchronise the TCP/IP settings with the Gigaset SX541 WLAN dsl (see page 37).

Installing Network Services

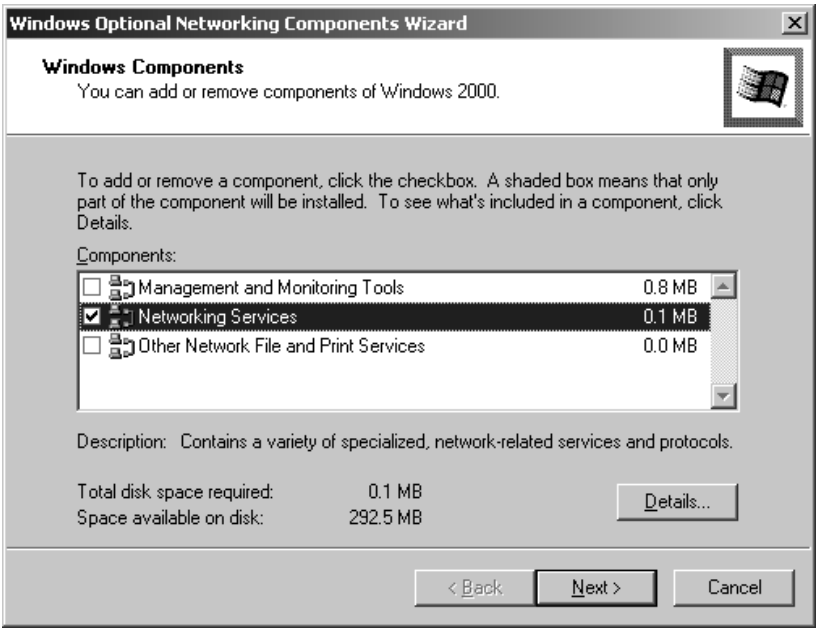
You have to install the network services so that the PCs in your network can access shared resources. This is done as follows:

➔ Click ***Start*** – ***Settings*** – ***Control Panel***.

➔ Double-click the ***Network and Dial-up connections*** icon.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
This folder contains network connections for this computer, and a wizard to help you create a new connection.
To create a new connection, click Make New Connection.
To open a connection, click its icon.
To access settings and components of a connection, right-click its icon and then click Properties.
To identify your computer on the network, click Network Identification.
To add additional networking components, click Add Network Components.
Select an item to view its description.
Name
Type
Status
Make New Connection
Local Area Connection
LAN
Network ca
2 object(s)

➔ In the left-hand pane click ***Add Network Components***.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 0.8 MB
Networking Services 0.1 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.1 MB
Space available on disk: 292.5 MB
Details...
< Back
Next >
Cancel

➔ Now select ***Networking Services*** and click ***Next***.

➔ You will now be prompted to insert the Windows installation CD. Insert the WIN2000 CD and click ***OK*** to install all the required components.

Selecting a Computer Name and Workgroup

You now have to specify a name for the PC and assign it to a workgroup.

➔ In the left-hand pane, click ***Network Identification*** and then on ***Properties***.

➔ In the ***Computer name*** field, enter the name the PC is to appear under in the network. This name must be unique within the network.

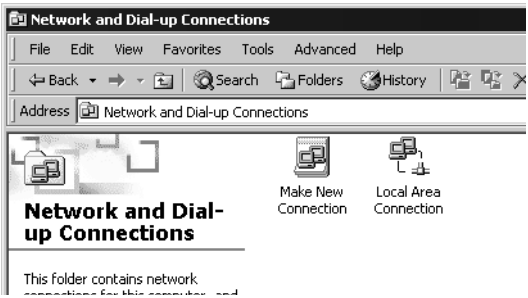
➔ In the ***Workgroup*** field, type a name for the workgroup. This name must be the same for all the PCs in the network.

➔ Confirm this with ***OK***.

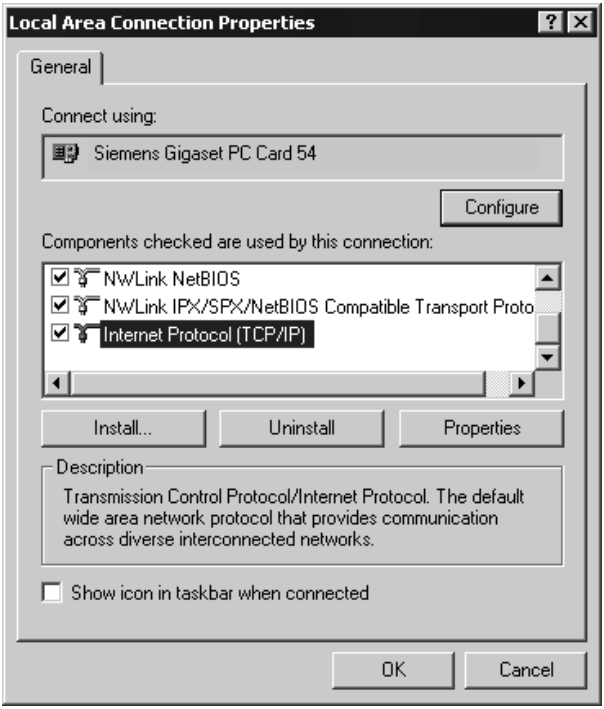
Installing the TCP/IP Protocol

The TCP/IP protocol ensures that the PCs in the network can communicate with each other. You now have to install this Protocol.

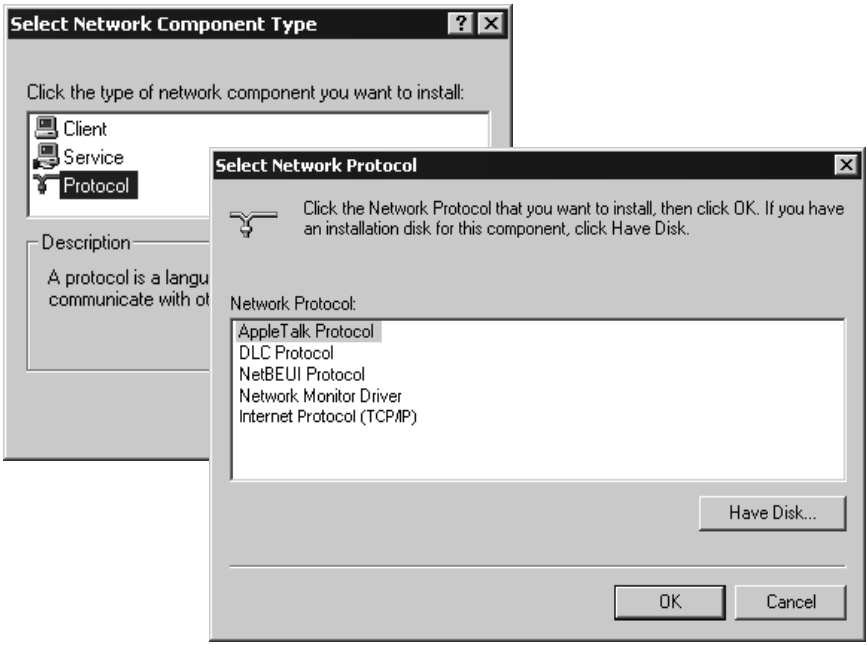
➔ Right click to open the ***LAN connection***.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Make New Connection
Local Area Connection
Network and Dial-up Connections
This folder contains network

➔ In the next window click ***Properties***.



➔ Click ***Install***.



➔ Now select ***Protocol*** and click ***Add***.

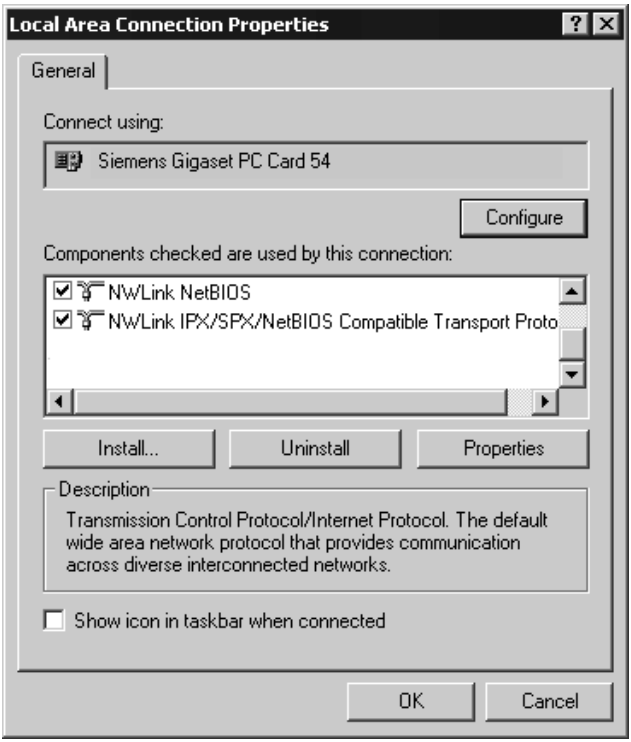
➔ In the ***Network Protocol*** list, select ***Internet Protocol (TCP/IP)***.

➔ Click ***OK***.

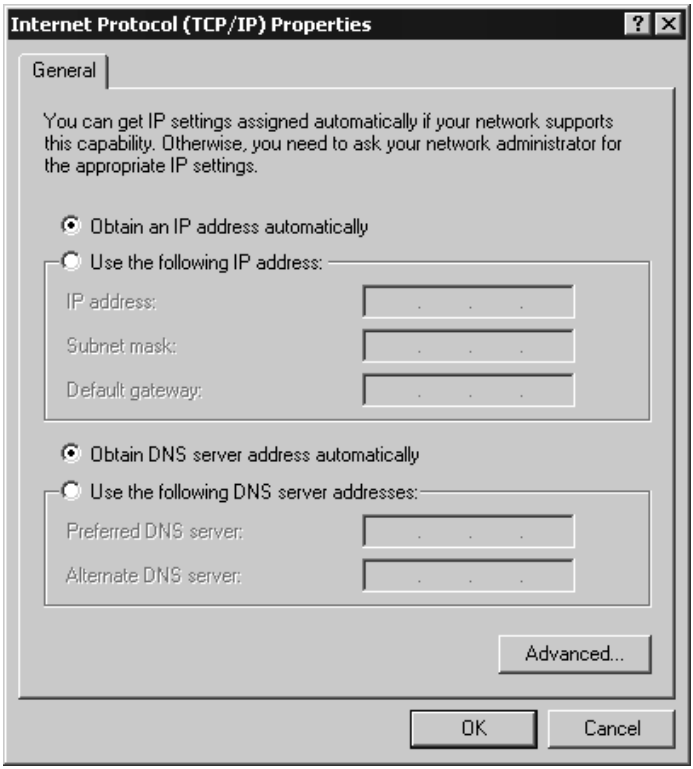
The TCP/IP protocol is now shown in the ***Local Area Connection Properties*** window.

TCP/IP Settings

The TCP/IP protocol requires certain settings which you should now make or check so that it can function smoothly.



➔ Select ***Internet Protocol (TCP/IP)*** and click ***Properties***.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

➔ If the ***Obtain IP address automatically*** and ***Obtain DNS server address automatically*** options have already been activated, your PC is already configured for DHCP. Click ***Cancel*** and close the following windows with ***OK*** to save your network configuration.

➔ If the ***Obtain IP address automatically*** and ***Obtain DNS server address automatically*** have not yet been activated, select them now and click ***OK***. Close the following screens.

Deactivating the HTTP Proxy

Make sure that the HTTP Proxy in your Web browser is deactivated. This function must be deactivated so that your Web browser can read your Gigaset SX541 WLAN dsl's configuration pages.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First decide which browser you are using and then follow the appropriate steps.

Internet Explorer

➔ Open Internet Explorer. Click ***Tools*** – ***Internet Options***.

➔ In the ***Internet Options*** window, click the ***Connections*** tab.

➔ Click ***LAN settings***.

➔ Deactivate all options in the ***Local Area Network (LAN) Settings*** window.

➔ Click ***OK*** and then ***OK*** again to close the ***Internet Options*** window.

Mozilla Firefox

➔ Open Mozilla Firefox. Click ***Tools*** and then on ***Settings***.

➔ In the ***Settings*** window, click ***Connection Settings...*** .

➔ In the ***Connection Settings*** window, select the option ***Direct connection to the Internet***.

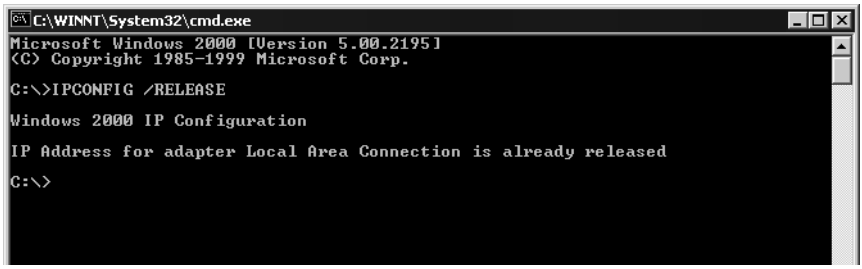
➔ Click ***OK*** to finish.

Synchronising the TCP/IP Settings with the Gigaset SX541 WLAN dsl

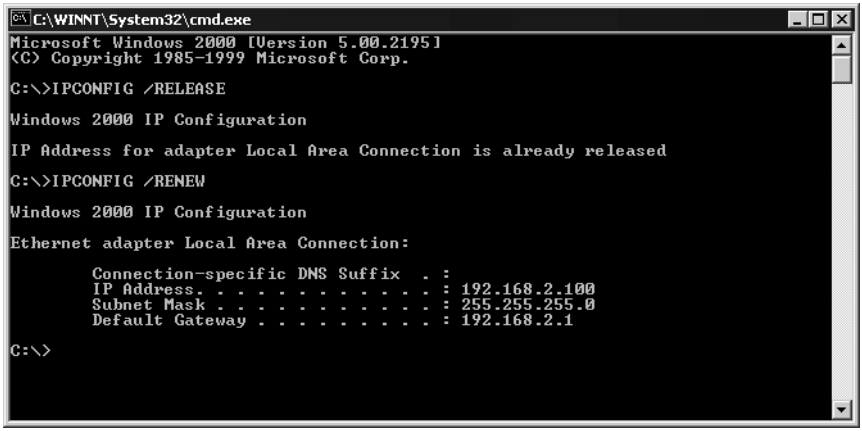
You have now configured your PC so that it is ready to be connected to the Gigaset SX541 WLAN dsl. You now have to release the old TCP/IP settings and synchronise them with the settings of your Gigaset SX541 WLAN dsl.

➔ On the Windows Desktop, click ***Start*** – ***Programs*** – ***Accessories*** – ***Command prompt***.

➔ In the ***Command prompt*** window, enter the **`ipconfig /release`** command and press the ENTER key.


C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP Address for adapter Local Area Connection is already released
C:\>

➔ Then enter the **`ipconfig /renew`** command and press the ENTER key.


C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP Address for adapter Local Area Connection is already released
C:\>IPCONFIG /RENEW
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
C:\>

If the default IP address (192.168.2.1) of the Gigaset SX541 WLAN dsl was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 255). The ***Subnet Mask*** must always be 255.255.255.0 and the ***Standard Gateway*** must have the IP address of the Gigaset SX541 WLAN dsl (192.168.2.1). These values confirm that your Gigaset SX541 WLAN dsl is working.

➔ Enter **`exit`** and press the ENTER key.

Network Configuration with Windows 98 SE, ME

To integrate a PC with Windows 98 SE or ME in a local network, you must carry out the following steps:

1. Set up the PC as a client for Microsoft networks (see below).
2. Select computer names and workgroup (see page 39).
3. Install the TCP/IP protocol (see page 40).
4. Make TCP/IP protocol settings (see page 41).
5. Deactivate the http proxy (see page 45).
6. Synchronise the TCP/IP settings with the Gigaset SX541 WLAN dsl (see page 46).

Setting up a PC as a Client for Microsoft Networks

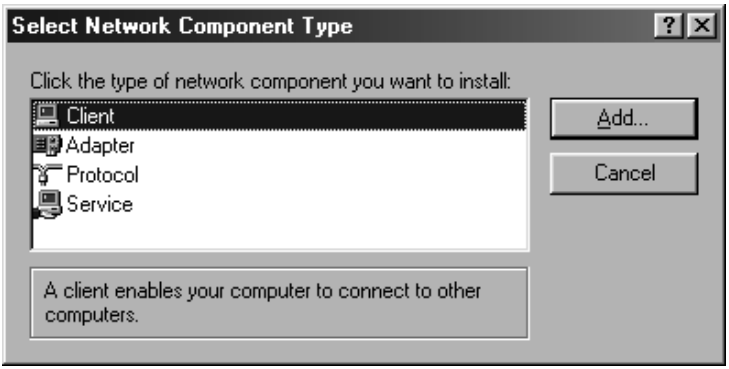
Before the PCs in your network can work together, you have to configure them as a Microsoft network Client. This is done as follows:

➔ Click ***Start*** – ***Settings*** – ***Control Panel***.

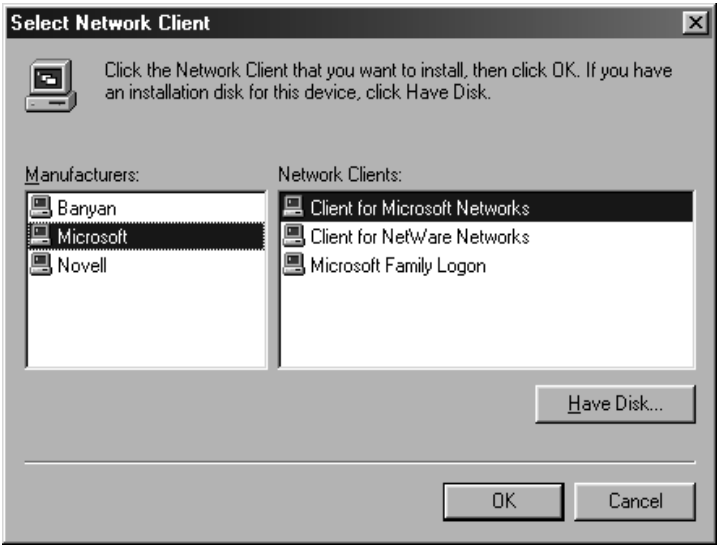
➔ Double-click the ***Network*** icon and then open the ***Configuration*** tab in the ***Network*** window.

➔ Check whether the list of components contains the entry ***Client for Microsoft Networks***.

➔ If it is not there click ***Add***.



➔ Select ***Clien***t as the network component type and click ***Add***.



➔ Under ***Manufacturer*** select ***Microsoft*** and under ***Network Clients*** select ***Client for Microsoft Networks***.

➔ Confirm this with ***OK***.

Selecting a Computer Name and Workgroup

You now have to specify a name for the PC and assign it to a workgroup.

➔ In the ***Network*** window, change from the ***Configuration*** tab to ***Identification***.

➔ In the ***Computer name*** field, enter the name the PC is to appear under in the network. This name must be unique within the network.

➔ In the ***Workgroup*** field, type a name for the workgroup. This name must be the same for all the PCs in the network.

The ***Description*** field can be left empty.

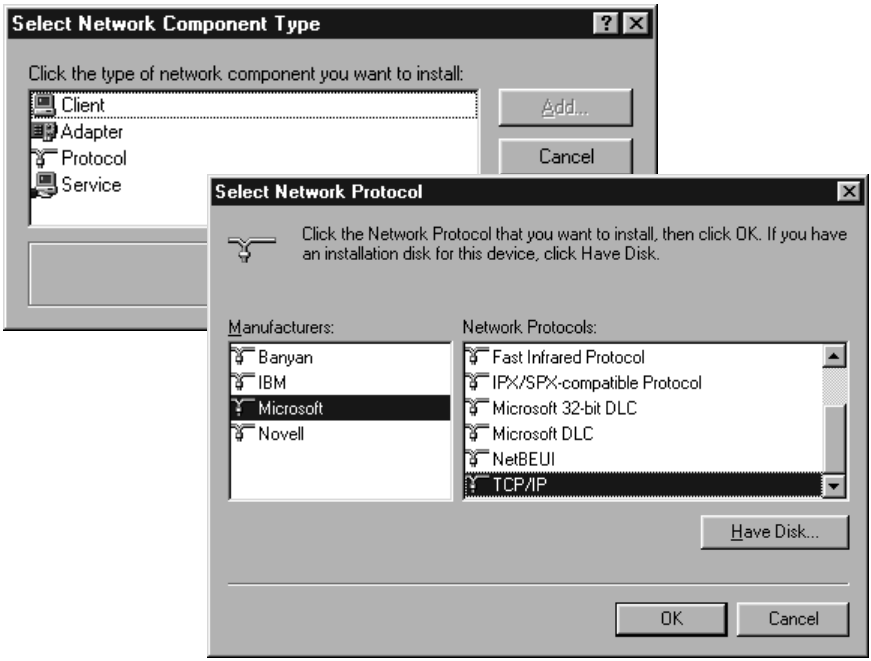
Installing the TCP/IP Protocol

The TCP/IP protocol ensures that the PCs in the network can communicate with each other. You must install this Protocol first for the network adapter that establishes the connection with the Gigaset SX541 WLAN dsl.

➔ In the ***Network*** window, change from the ***Identification*** tab to ***Configuration***.

➔ In the ***Network*** window, check that there is a TCP/IP -> entry for your network card or network adapter in the list of components. If, for example, you are using a Gigaset PC Card as the wireless network adapter, the list must contain the entry ***TCP/IP > Siemens Gigaset PC Card***

➔ If the entry does not exist, click ***Add***.



➔ Select ***Protocol*** as the network component type and click ***Add***.

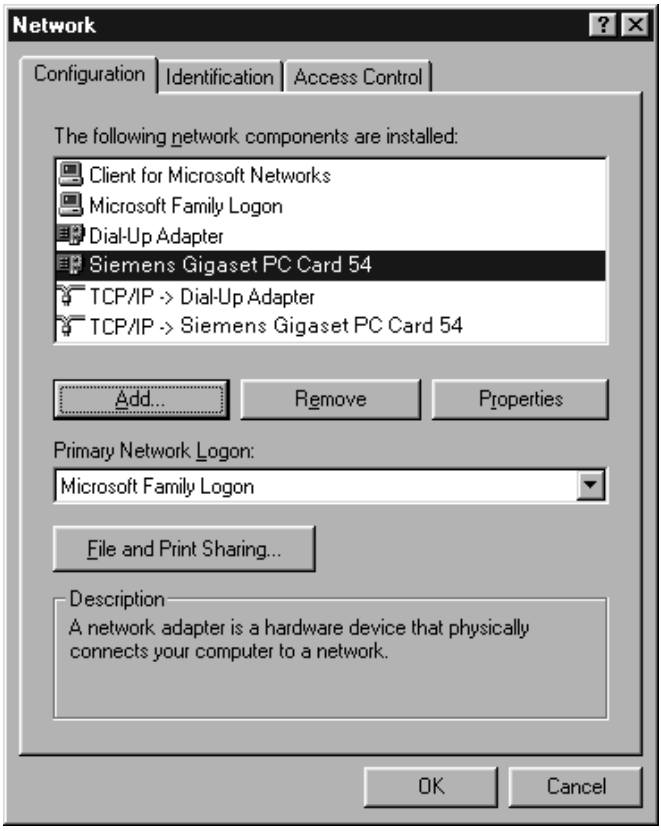
➔ Under ***Manufacturer*** select ***Microsoft*** and under ***Network protocol*** select ***TCP/IP*** and click ***OK*** to confirm.

Making TCP/IP Settings

The TCP/IP protocol requires certain settings which you should now make so that it can function smoothly.

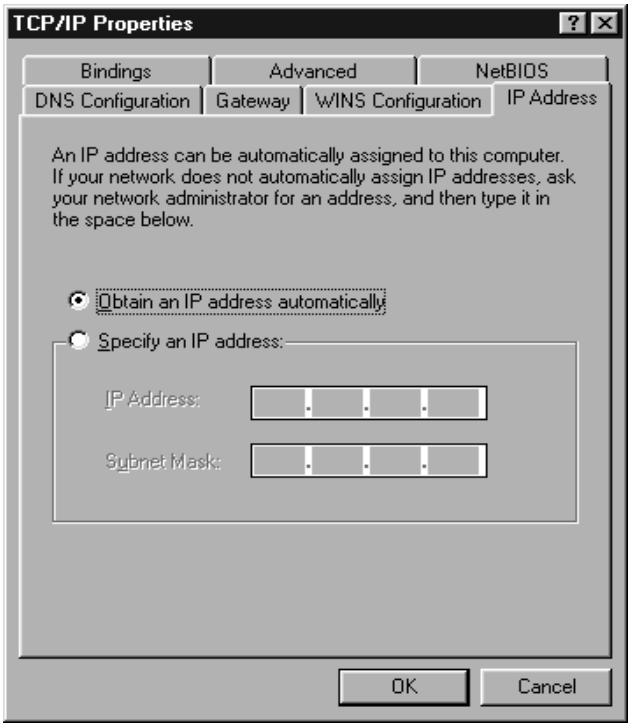
➔ In the ***Network*** window, change to the ***Configuration*** tab.

➔ Select the ***TCP/IP >*** entry for your network card.



➔ Click ***Properties***.

➔ Open the ***IP Address*** tab.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

➔ If ***Obtain IP address automatically*** has already been activated, your PC is already configured for DHCP. Click ***Cancel*** and close the following windows with ***OK*** to start your network configuration.

You may be prompted to insert your Windows Installation CD. Follow the instructions in the installation procedure.

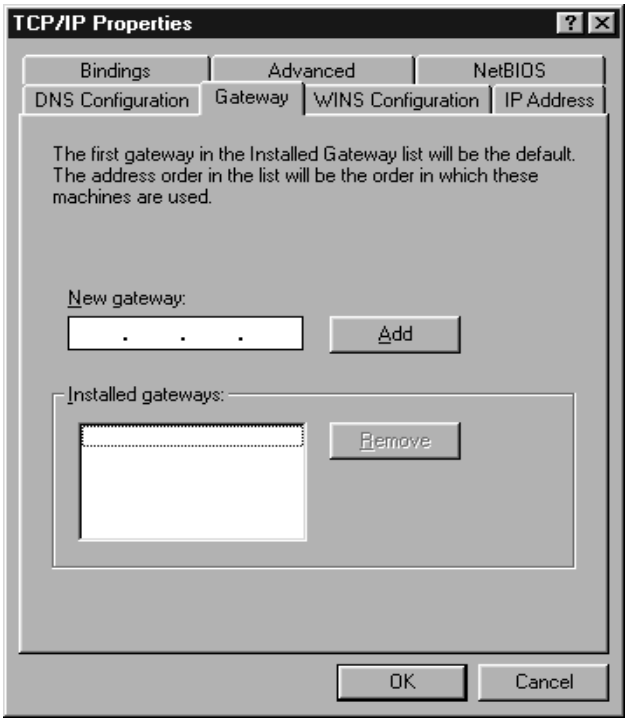
Once the copying procedure is completed, you will be prompted to reboot your system.

➔ Click ***Yes***. The PC will then be rebooted.

Then read on from page 45.

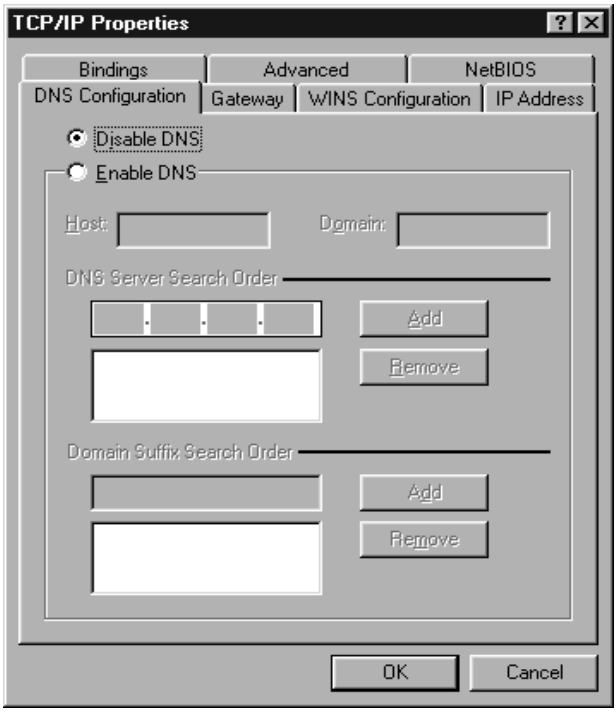
➔ If ***Obtain IP address automatically*** has not been activated, activate this option now.

➔ Open the ***Gateway*** tab and remove any entries in the ***Installed gateways*** list.



➔ Open the ***DNS Configuration*** tab.

➔ Select ***Disable DNS***.



➔ Click ***OK***.

➔ Finish the network configuration with ***OK***.

You may be prompted to insert your Windows Installation CD. Follow the instructions in the installation procedure.

Once the copying procedure is completed, you will be prompted to reboot your system.

➔ Click ***Yes***. The PC will then be rebooted.

Deactivating the HTTP Proxy

Make sure that the HTTP Proxy in your Web browser is deactivated. This function must be deactivated so that your Web browser can access your Gigaset SX541 WLAN dsl's configuration pages.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First decide which browser you are using and then follow the appropriate steps.

Internet Explorer

➔ Open Internet Explorer. Click ***Tools*** – ***Internet Options***.

➔ In the ***Internet Options*** window, click the ***Connections*** tab.

➔ Click ***LAN settings***.

➔ Deactivate all options in the ***Local Area Network (LAN) Settings*** window and click ***OK***.

➔ Click ***OK*** again to close the ***Internet Options*** window.

Mozilla Firefox

➔ Open Mozilla Firefox. Click ***Tools*** and then on ***Settings***.

➔ In the ***Settings*** window, click ***Connection Settings...*** .

➔ In the ***Connection Settings*** window, select the option ***Direct connection to the Internet***.

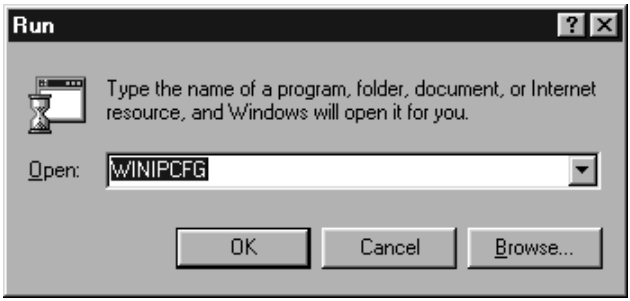
➔ Click ***OK*** to finish.

Synchronising the TCP/IP Settings with the Gigaset SX541 WLAN dsl

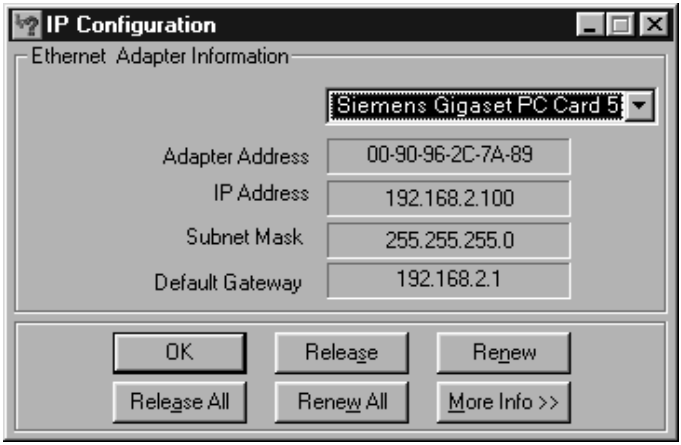
You have now configured your PC so that it is ready to be connected to the Gigaset SX541 WLAN dsl. You now have to release the old TCP/IP settings and synchronise them with the settings of your Gigaset SX541 WLAN dsl.

➔ Click ***Start*** – ***Run***.

➔ Type **`WINIPCFG`** and click ***OK***.



There may be a slight delay before the ***IP Configuration*** window appears.



➔ Select your network adapter from the selection list.

➔ Click ***Release*** and then on ***Update***.

If the default IP address (192.168.2.1) of the Gigaset SX541 WLAN dsl was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 255). The ***Subnet Mask*** must always be 255.255.255.0 and the ***Standard Gateway*** must have the IP address of the Gigaset SX541 WLAN dsl (192.168.2.1). These values confirm that your Gigaset SX541 WLAN dsl is working.

➔ Click ***OK*** to close the ***IP Configuration*** window.

Checking the Connection to the Gigaset SX541 WLAN dsl

Once the network has been set up on your PC, you can check whether the PC is correctly connected to the Gigaset SX541 WLAN dsl. This can be done as follows:

➔ Open ***Command prompt***. To do this, click ***Start*** – ***Programs*** – ***Command prompt***.

➔ Enter the command **`ping 192.168.2.1`**.

> **Please remember:**
> 192.168.2.1 is the default IP address for the Gigaset SX541 WLAN dsl.
> If the IP address was changed, enter the new IP address.

The **`ping`** command sends data packets to the Gigaset SX541 WLAN dsl with the specified IP address and checks whether the router responds. If this is the case, the command presents statistics about the connection, for example how many data packets were sent, how many were received, how long the transfer took, etc. If you can see this information, then the connection to the router is functioning properly.

If the command does not return any statistics, but ends with a time-out, this means that the components cannot communicate with each other. Check the following points:

1. Is the Ethernet cable between the Gigaset SX541 WLAN dsl and the PC correctly connected or is there a wireless connection via a wireless network adapter?

   The LED display for the LAN connections on the Gigaset SX541 WLAN dsl and link display for the network card in your PC must be illuminated. For wireless connections, the Gigaset WLAN Adapter Monitor must display connection information.

2. Has TCP/IP been properly configured on your PC?

   If the Gigaset SX541 WLAN dsl has the IP address 192.168.2.1, your PC's IP address must be between 192.168.2.2 and 192.168.2.255. The default gateway must have the address 192.168.2.1.

If you can successfully address the Gigaset SX541 WLAN dsl with the **`ping`** command, then the PC has been configured correctly.

The User Interface

Once you have configured the network settings on a PC in your local network, you can then use that PC to configure the Gigaset SX541 WLAN dsl with the Gigaset SX541 WLAN dsl's user interface. You can use any browser for the configuration, for example Microsoft Internet Explorer 6.0 or higher, Mozilla Firefox 1.0 or higher.

Please remember:

To start the configuration environment you might need to deactivate the HTTP proxy for your browser (see page 45 for Windows 98 SE/ ME, page 28 for Windows XP and page 36 for Windows 2000).

If you use Windows XP Service Pack 2 you need to configure the popup blocker (see page 28).

Launching the User Interface

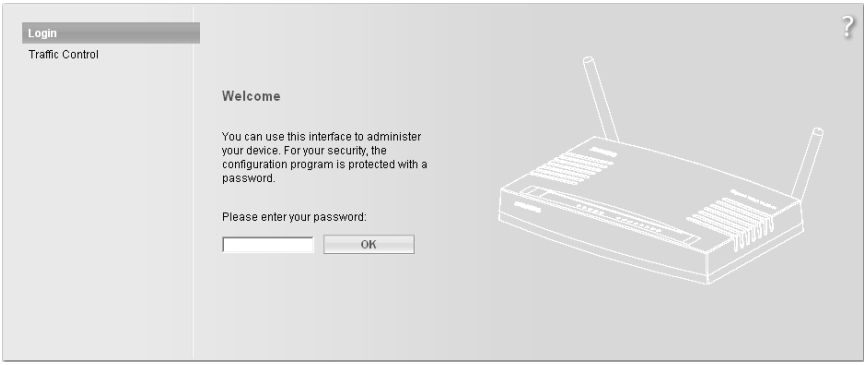
To access the Gigaset SX541 WLAN dsl's user interface:

➔ Launch your Web browser.

➔ Enter the IP address of the Gigaset SX541 WLAN dsl in the browser's address field.

`http://sx541` or **`http://192.168.2.1`**

The login screen appears:


Login
Traffic Control
Welcome
You can use this interface to administer your device. For your security, the configuration program is protected with a password.
Please enter your password:
OK

For your security, the configuration program is protected with a password. In the default setting, this password is ***admin***.

➔ Type in this password and click ***OK***.

Please remember:

For security reasons you should change this password at a later stage (see page 60).

A screen with security information is displayed.

For the initial configuration you can skip this information. If you carry out all the basic and security settings using the wizard as described below, then your device and network are fully protected. If not, the next time you log on you will be informed of security gaps in the configuration program.

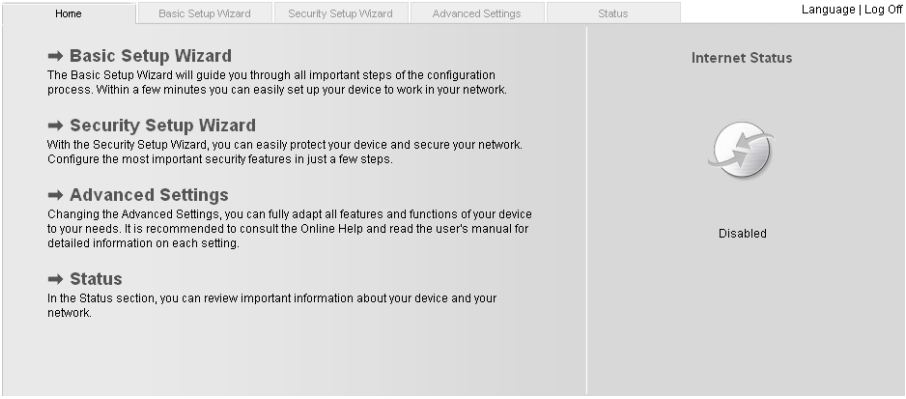
➔ Click ***OK***.

You will now see the start screen.

Note:
You will find information about the currently used and available time and data volume for your Internet connection by clicking on ***Traffic Control***. There is more detailed information about this in the section entitled "Traffic Control" on page 133.

The Start Screen

The start screen is the starting point for all configuration and administration activities.


Home
Basic Setup Wizard
Security Setup Wizard
Advanced Settings
Status
Language | Log Off
➡ Basic Setup Wizard
The Basic Setup Wizard will guide you through all important steps of the configuration process. Within a few minutes you can easily set up your device to work in your network.
➡ Security Setup Wizard
With the Security Setup Wizard, you can easily protect your device and secure your network. Configure the most important security features in just a few steps.
➡ Advanced Settings
Changing the Advanced Settings, you can fully adapt all features and functions of your device to your needs. It is recommended to consult the Online Help and read the user's manual for detailed information on each setting.
➡ Status
In the Status section, you can review important information about your device and your network.
Internet Status
Disabled

Start screen functions

On the start screen you can

- select the language for the user interface (see page 51),
- connect to the Internet (see page 123),
- open the Status menu to obtain status information about the Gigaset SX541 WLAN dsl (see page 118),
- call up the wizard for the basic configuration: Basic Setup Wizard (see page 53),
- call up the Security Setup Wizard (see page 59),
- open the Advanced Settings menu for additional configuration options (see page 68).

You can call up the wizards, the Advanced settings menu and status information from any other configuration program screen at any time via the tabs at the upper margin of the user interface.

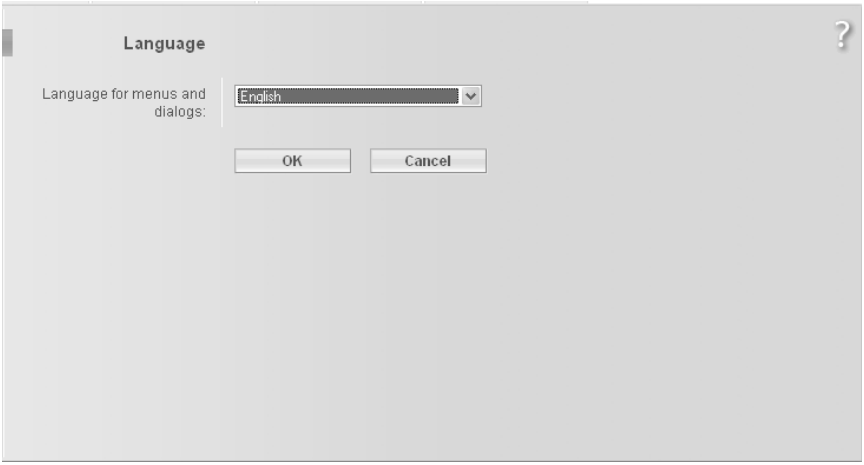
The configuration program offers you the following functions:

Basic Setup Wizard	Use this wizard for the settings required for connecting to the Internet. You can set data for your region and configure Internet telephony. This is described from page 53.
Security Setup Wizard	This wizard allows you to take precautions against unauthorised access to your Gigaset SX541 WLAN dsl and the local network. For example, you can assign a password and set up encryption for wireless traffic. This is described from page 59. For the protection of your network we recommend that you carry out this setup.
Advanced Settings	Additional functions are offered in the Advanced Settings menu. For example, you can configure your fixed network/ Internet telephony connection, back up and restore your configuration data, set up your Gigaset SX541 WLAN dsl as a virtual server for your network and much more. These configuration steps are optional and can be carried out at a later stage. This is described from page 68.
Status	You can view information about the configuration and status of your Gigaset SX541 WLAN dsl in the Status menu. This is described from page 127.
Internet status	You can view the status of your Internet connection and establish a manual connection to the Internet (see page 118).
Language	You can select the language for the user interface (see page 51).

Selecting a Language

The user interface can be presented in various languages.

➔ Click ***Language*** on the top right of the screen.



➔ If you wish to change the preset language, select the required language from the list.

➔ Click ***OK*** to apply the setting.

You might have to load the file for the language you require. Follow the on-screen instructions on the user interface.

Reboot the device to activate the change. Confirm the reboot in the dialogue field shown.

Once the procedure has been concluded the start screen is shown again.

Elements on the User Interface

The user interface pages contain the following elements:

Log Off button

The ***Log Off*** button is always present on the right of the user interface. If you click ***Log Off*** the session is terminated and the login screen appears again.

Help

click the question mark to display explanations about the current user interface screen.

Buttons and symbols used by the wizards

The wizards use graphic symbols to show which steps you have already carried out.

As soon as you have changed the configuration in a screen, you can activate the new setting by clicking on ***Next >*** at the bottom of the screen. The ***< Back*** button returns you to the previous configuration step and ***Cancel*** returns you to the start screen.

Buttons in the Advanced Settings menu

OK	Transfers the settings you have made to the Gigaset SX541 WLAN dsl configuration.
Cancel	Deletes all the entries in a screen since the last time you clicked on ***OK***. This button is not available for the initial configuration of the device.

Other buttons may be visible depending on the function in question. These are described in the relevant sections.

Basic Setup Wizard

The Basic Setup Wizard guides you step by step through the general configuration of the Gigaset SX541 WLAN dsl. This includes settings for your region and for your Internet access.

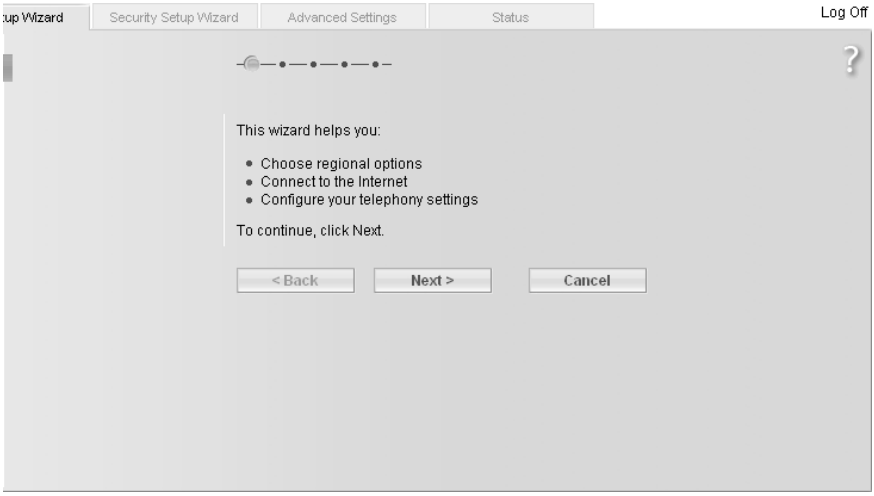
Connection to the Internet is established via the Gigaset SX541 WLAN dsl for all PCs connected to it. You need your Internet Provider's access data for the configuration. Please have this data to hand.

Please remember:

The Basic Setup Wizard will reconfigure your Internet settings if this has already been done previously. This does not affect the WLAN and LAN settings.

The access data is stored in the Gigaset SX541 WLAN dsl during configuration. Before passing the device on to somebody else or having your dealer replace it, you should first restore the factory settings (see page 124). Otherwise unauthorised persons may use your Internet access data at your expense.

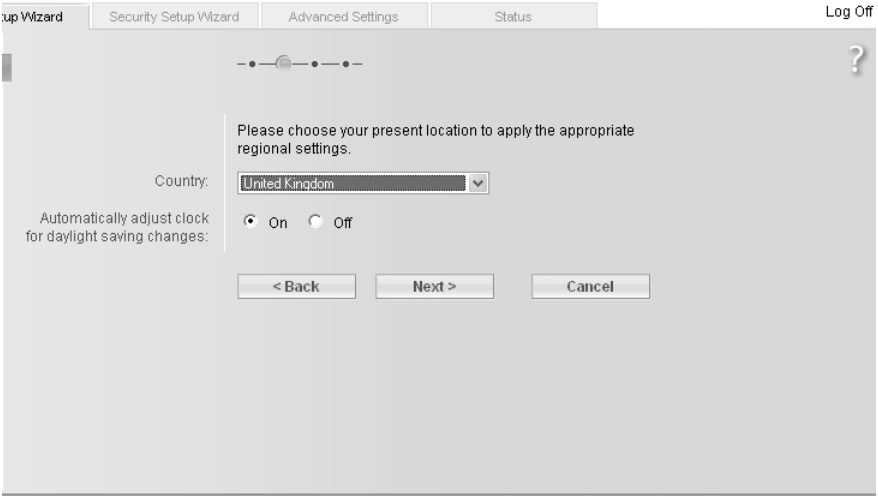
➔ Select ***Basic Setup Wizard*** on the start screen to start the configuration.



➔ Click ***Next >***.

Regional Options

You can select your present location for the regional settings on this screen.



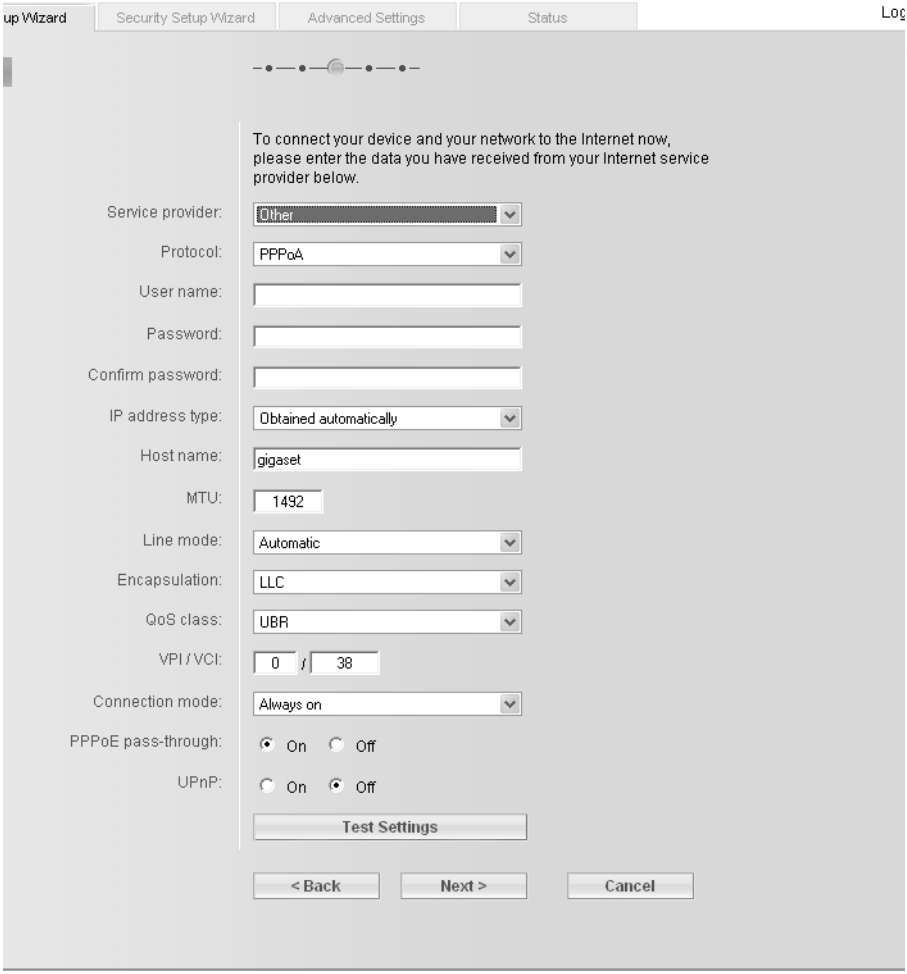
➔ Select the country where you are currently located from the list. You can make the settings for the clock to change automatically to summer time and/or to the time zone as you wish.

➔ Select the required option and/or select the time zone for your location.

➔ Click ***Next >***.

Configuring Internet Connections

You will find the access data you need for configuring the Internet connection in the documentation received from your Internet Provider (ISP).



➔ Select the option ***Other*** from the ***Service provider*** selection menu.

➔ Enter the data you have been given by your Internet provider: ***Protocol***, ***User name*** and ***Password***.

Leave the default settings for the parameters ***IP address type***, ***Host name***, ***MTU***, ***Line mode***, ***Encapsulation***, ***QoS class*** and ***VPI / VCI*** unless you have been given other data by your service provider.

Please remember:
Connection to the Internet is only possible if you have entered all the data for your Internet provider correctly.

➔ Select how Internet sessions are to be established via ***Connection mode***:

– Select ***Always on*** if the connection is to exist at all times when the Gigaset SX541 WLAN dsl is switched on.

Please remember:
This option can result in high connection charges if you have a time-based tariff.

– Select ***Connect on demand*** if applications such as a Web browser or an e-mail program are to connect to the Internet automatically.

– In the ***Idle time before disconnect*** field, enter a period of time after which the Internet connection is to be automatically ended if no data is transmitted (default setting: 3 minutes).

You can deactivate this function by entering "0". This means that the connection will continue to exist even if no data is transmitted. If you have a time-based tariff this can cause high charges. In this case you should enter a value other than "0".

This time setting only applies to the ***Connect on request*** option.

– Select ***Connect manually*** if you always want to establish and end the connection to the Internet manually. If you have a time-based tariff this will save you high connection charges. How to establish a connection manually is described on page 123.

Please remember:
You must set the option ***Always on*** if you want to operate Internet telephony.

➔ Click ***Test Settings*** to check the Internet connection. The router will attempt to connect to the Internet. Any Internet connection already in existence will be closed first.

You will find information about the test steps and results on the ***Internet Connection Test*** screen.

PPPoE pass-through

PPPoE pass-through enables you to use an additional Internet connection (with another service provider) from one PC. You can find detailed information about this on page 75.

➔ Deactivate ***PPPoE pass-through*** if you do not wish to use this function.

➔ When you have entered the data, click ***Next >***.

Using UPnP (Universal Plug and Play)

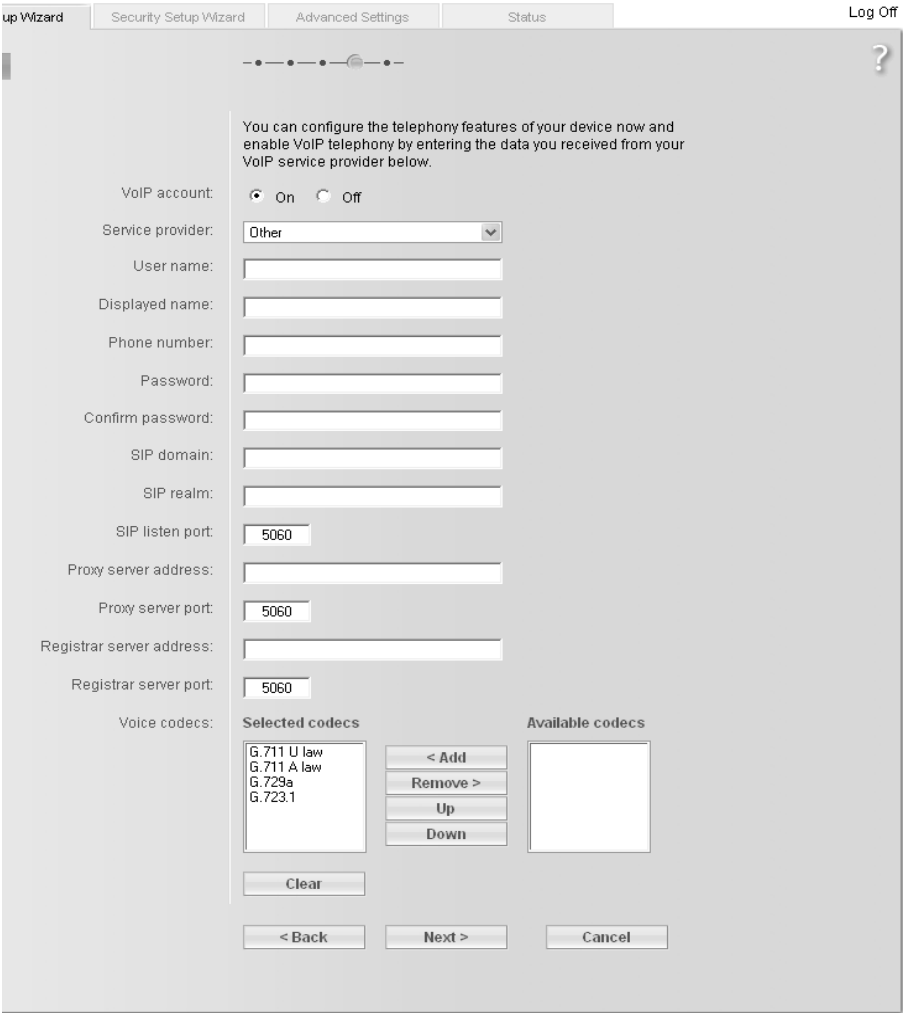
PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered on the network. You can find detailed information about this on page 73.

➔ Activate ***UPnP*** if you wish to use this function.

➔ Click ***Next >***.

Telephony

You will find the access data you need for configuring the Internet telephony (VoIP) in the documentation received from your service provider.



➔ Select ***On*** for ***VoIP account***, if you want to use Internet telephony (default setting).

➔ Select ***Other*** from the ***Service provider*** selection menu (default setting).

➔ Enter the data you have been given by your service provider:

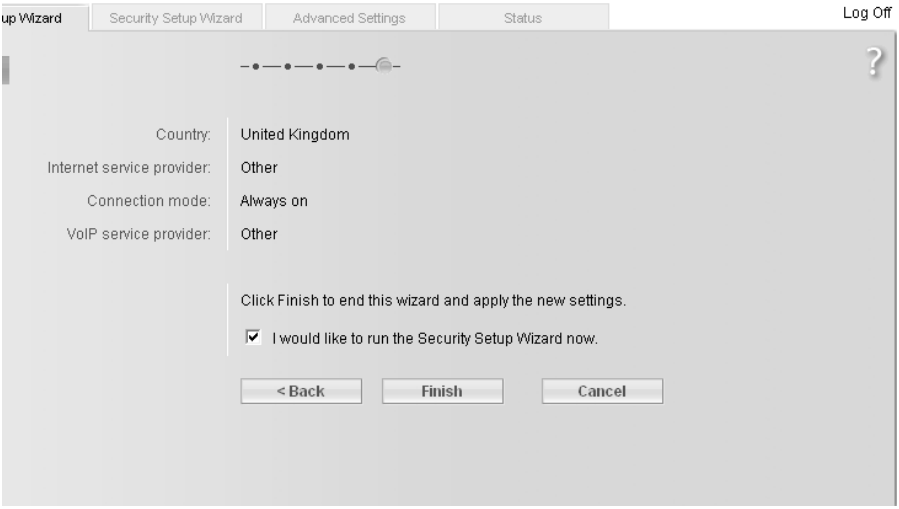
User name, ***Displayed name***, ***Phone number***, ***Password***, ***SIP domain***, ***SIP realm***, ***Proxy server address and Registrar server address***.

➔ Leave the default settings for the parameters ***SIP listen port***, ***Proxy server port***, ***Registrar server port*** and ***Voice codecs*** unless you have been given other data by your service provider.

➔ Confirm your selection with ***Next >***.

Summary

The basic settings you have made through the wizard are shown for you to check in the next step.



➔ If you want to make changes to the settings, click ***< Back***.

➔ If you want to confirm the settings, click ***Finish*** to close the basic setup wizard.

You will then be taken automatically to the start screen for the ***Security Setup Wizard***. If you want to carry this out at a later stage, deactivate the option ***I would like to run the Security Setup Wizard now.***

The Gigaset SX541 WLAN dsl is now configured and ready to connect to the Internet.

Security Settings

The ***Security Setup Wizard*** offers you additional settings for improving your network security. You can

- assign a password for configuring the Gigaset SX541 WLAN dsl (see page 60),
- change the ID for your wireless network (SSID) (see page 61),
- set the Encryption for wireless traffic (see page 62),
- limit access to your wireless network to certain PCs (see page 75).

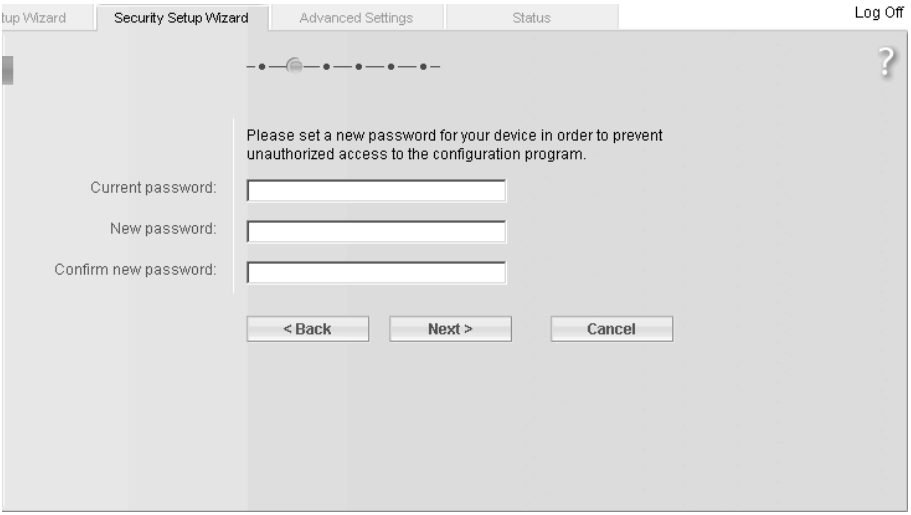
The Gigaset SX541 WLAN dsl's user interface will guide you through the security configuration step by step. Once you have completed a screen, click ***Next >***. If you want to make any changes or check your entries, click ***< Back***.

➔ Select ***Security Setup Wizard*** on the start screen or on the tab to start the security configuration if you did not go straight to the start screen for the security settings after making the basic settings.

➔ Click ***Next >*** to continue.

Assigning a Password

In the first step of the setup you can change the password for the user interface. When supplied, the configuration of your Gigaset SX541 WLAN dsl is protected with the password ***admin***. To prevent unauthorised changes to the configuration, you should change this password from time to time.



➔ Enter the old password in the ***Current password*** field.

➔ Enter a new password in the ***New password*** field, and repeat it in the ***Confirm new password*** field.

The password can be up to 12 alphanumerical characters long. Avoid proper names and all too obvious words. Mix letters and numbers together.

Please remember:

If you ever forget your password you will have to reset your Gigaset SX541 WLAN dsl (see page 18). Please bear in mind that this will restore **all** the settings to the factory configuration. No password will be active either.

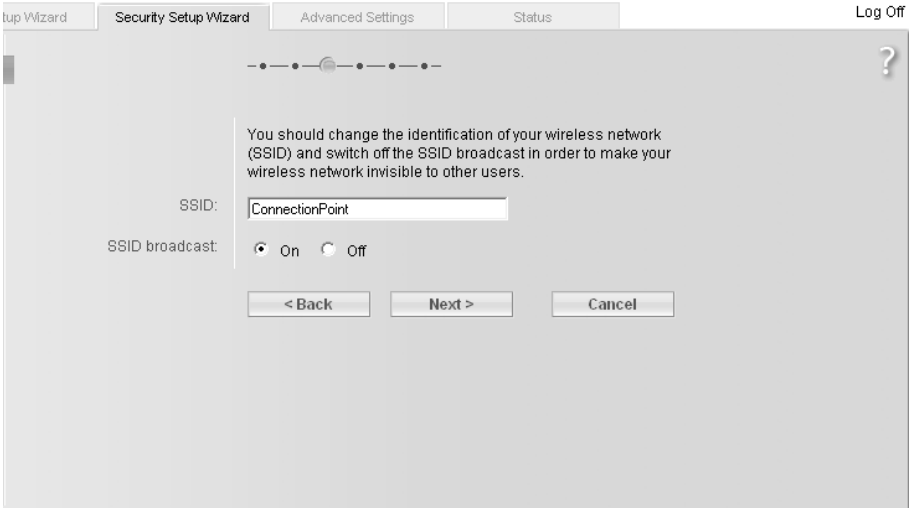
◆ To go to the next step, click on ***Next >***.

SSID

Before the wireless network components can communicate with each other, you must use the same SSID (Service Set Identifier).

The default SSID for the Gigaset SX541 WLAN dsl is **ConnectionPoint**. For security reasons you should change this SSID and deactivate SSID broadcast.

If this option is enabled, the Gigaset SX541 WLAN dsl will send the SSID in all data transmissions and your Gigaset SX541 WLAN dsl's SSID will be displayed on PCs that have a wireless network adapter. In this case, unauthorised persons could use the SSID to gain access to your network.



➔ Enter a character string of your choice in the ***SSID*** field. The SSID is case sensitive. It can be up to 32 alphanumerical characters long.

> **Please remember:**
> The connection to the wireless network adapters will be interrupted until the new SSID has been entered in them as well.

➔ Deactivate the option ***SSID broadcast*** and make a note of the SSID. You will need this to log on your PC.

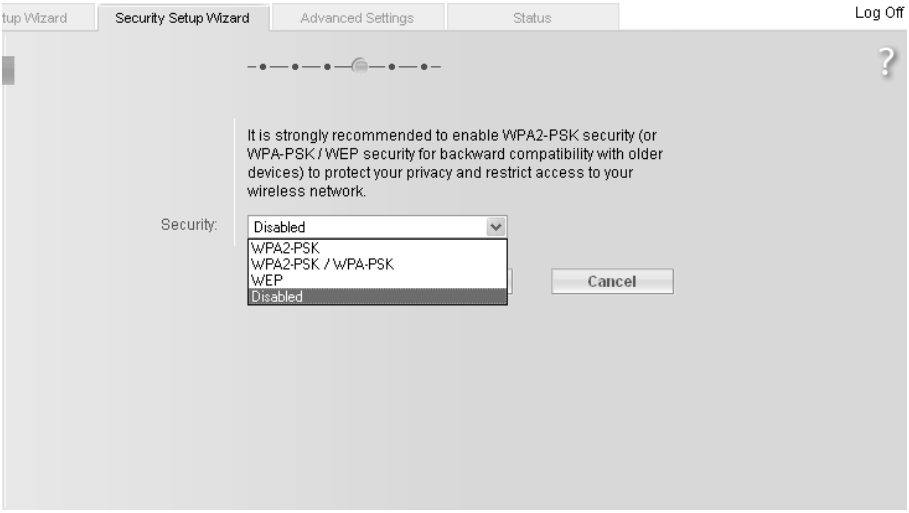
➔ Click ***Next >*** to proceed to the next step.

Setting Security Functions for the Wireless Network

In the next step you can set the encryption and authentication methods for your wireless network.

Wireless networks are even more strongly exposed to the risk of eavesdropping than wired networks. With conventional network adapters an intruder only needs a device with a WLAN adapter (for example a Notebook or a PDA (Personal Digital Assistant)) with an appropriately configured network card in order to eavesdrop on every communication made via a nearby wireless LAN.

The Gigaset SX541 WLAN dsl makes use of effective encryption methods to prevent unauthorised eavesdropping as far as possible.



You can use the following security mechanisms:

- WPA2-PSK or WPA2-PSK / WPA-PSK (see page 63)
- WEP encryption (Wired Equivalent Privacy, see page 64)

We recommend using WPA2-PSK if it is supported by all components in your wireless network.

You will find further options for setting data encryption and authentication in the Advanced Settings menu (see page 97).

WPA2 / WPA with Pre-Shared Key (PSK)

WPA is a more advanced procedure than WEP for protecting wireless networks. Dynamic keys based on TKIP (Temporal Key Integration Protocol) offer increased security. The new standard WPA2 uses AES for the encryption.

WPA-PSK is a special WPA mode for users at home and in small companies without a company authentication server. Encryption keys are automatically generated with the Pre-shared Key, automatically changed ("rekeying") and authenticated between the devices after a certain period of time (Rekey Interval).

Please remember:

Every PC (network adapter) that requires access to a wireless network protected by WPA must also support WPA. To find out whether and how you can use WPA on your PC, read your network adapter's operating instructions.

➡ Select the ***WPA2-PSK*** option if it is supported by all components in your wireless network.

or

➡ Select the ***WPA2-PSK / WPA-PSK*** option if some or all components in your wireless network support WPA with the TKIP protocol.

Security Setup Wizard
Advanced Settings
Status
Log Off
It is strongly recommended to enable WPA2-PSK security (or WPA-PSK / WEP security for backward compatibility with older devices) to protect your privacy and restrict access to your wireless network.
Security:
WPA2-PSK
Pre-shared key:
Confirm pre-shared key:
< Back
Next >
Cancel

➡ Enter a key of your choice in the ***Pre-shared key*** field (min. 8 to max. 63 characters) and confirm it by repeating the entry.

You must also set the same Pre-shared Key for all wirelessly connected PCs.

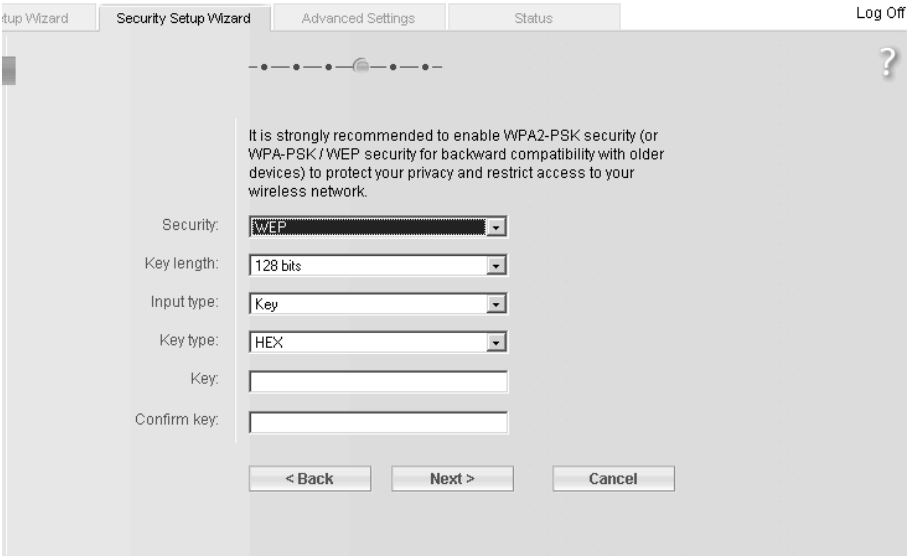
➡ To go to the next step, click ***Next >***.

WEP Encryption

WEP (Wired Equivalent Privacy) is an encryption procedure for radio signals in wireless networks and meets the IEEE 802.11 standard.

If you transmit data wirelessly and not all components in your wireless network support the higher security standard WPA (see page 63), we recommend that you activate WEP-Encryption for these network components.

You can choose either the standard 64-bit key or the more robust 128-bit key for encryption. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for the Gigaset SX541 WLAN dsl and all your wireless network adapters.



➔ Select the ***Key length***: 64 bits or 128 bits.

➔ Select the ***Input type***, i.e. whether you wish to enter the key manually or have it generated automatically by means of a ***Passphrase***.

Manual key entry

➔ Select the ***Key type***, ***Hex*** or ***ASCII***.

If you select ***Hex,*** you can use the characters **0** to **9** and **A** to **F**.

– With a 64-bit encryption depth, the key is exactly 10 characters long.
– With a 128-bit encryption depth, the key is exactly 26 characters long.

If you select ***ASCII*** you can use the characters **0** to **9**, **A** to **Z** and **a** to **z** plus the special characters in the ASCII character set.

– With a 64-bit encryption depth, the key is exactly 5 characters long.
– With a 128-bit encryption depth, the key is exactly 13 characters long.

➔ Confirm the key by entering it again in the ***Confirm key*** field.

Generating the key by means of a Passphrase

➔ Enter a ***Passphrase*** (up to 32 characters) and confirm it by entering it again. The key is generated automatically.

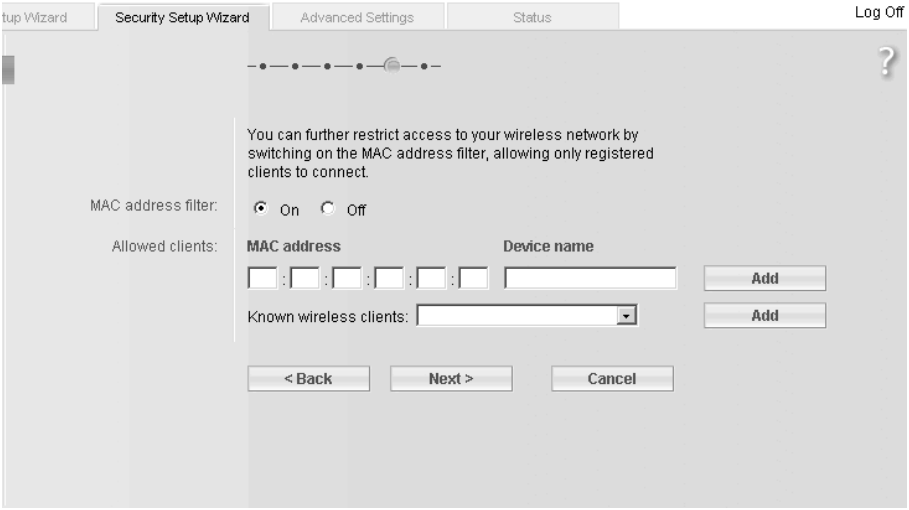
Please remember:

- It is very **important** that you make a note of the key or passphrase. You will need this information to configure the wireless network adapters properly.
- When you have concluded the Security Setup Wizard, you must change the WEP encryption on the wireless network adapters for the connected PCs in the same way as they will not otherwise be given access to the Gigaset SX541 WLAN dsl's wireless network.

➔ To go to the next step in the Security Setup Wizard, click ***Next >***.

Access Control Within the Wireless Network

you can specify which PCs will have wireless access to the Gigaset SX541 WLAN dsl and hence to your LAN in this step. The access control is based on the MAC address of the PCs' network adapters. You can enter the MAC addresses for the PCs manually or select them from the list of PCs that are currently logged in.



The default setting for access control is disabled. This means that all PCs that use the correct SSID can log in.

➔ Next to ***MAC address filter*** select the option ***On*** to activate the MAC filtering.

Entering MAC addresses manually

➔ Enter the MAC address of the network adapter. You will find this address on the bottom of the device.

➔ Enter the name of the PC.

➔ Click the ***Add*** button to add the entry to the list.

Selecting from the list of logged-in PCs

➔ Select the required PC from the ***Known wireless clients*** list. All PCs that are currently logged in to the router with the correct SSID are displayed.

➔ Click the ***Add*** button to add the selected PC to the list.

Please remember:

If you activate MAC access control, you must at least enter the PC from which you are configuring the Gigaset SX541 WLAN dsl. Otherwise you will no longer be able to access the user interface and a corresponding error message will be shown.

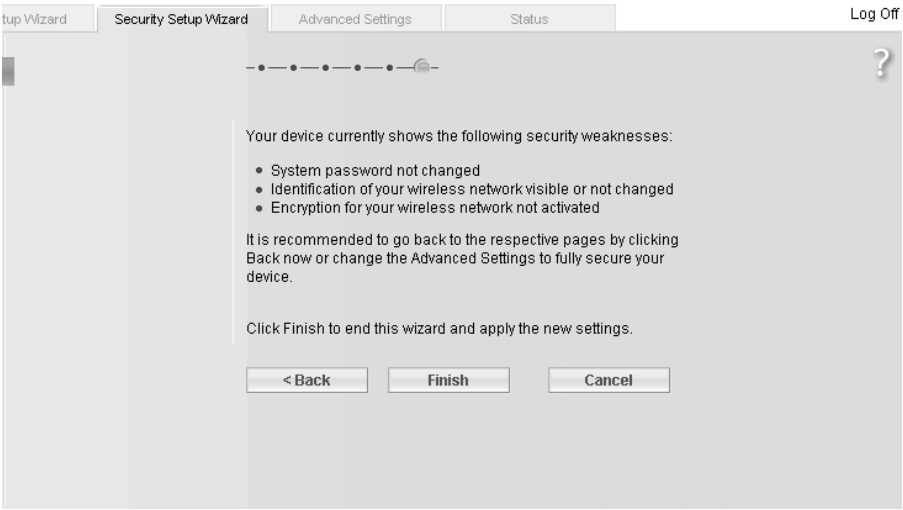
If, by mistake, you have denied all PCs access to the Gigaset SX541 WLAN dsl, you have two choices:

- You can completely reset the Gigaset SX541 WLAN dsl (see page 18).
- You can connect a PC to the Gigaset SX541 WLAN dsl using one of the LAN connections (by cable). As MAC access control only applies to PCs that are connected "wirelessly", you can use this PC to change the configuration.

➔ To go to the next step, click ***Next >***.

Saving Settings

On the next screen you conclude the wizard and save the settings. You will be informed of any security risks that still exist.


tup Wizard
Security Setup Wizard
Advanced Settings
Status
Log Off
?
Your device currently shows the following security weaknesses:
System password not changed
Identification of your wireless network visible or not changed
Encryption for your wireless network not activated
It is recommended to go back to the respective pages by clicking Back now or change the Advanced Settings to fully secure your device.
Click Finish to end this wizard and apply the new settings.
< Back
Finish
Cancel

➔ Click ***Finish*** to conclude the wizard.

The settings will now be active on your Gigaset SX541 WLAN dsl.

Please remember:

You must now configure WEP or WPA key for your PC's wireless network adapter if this has been configured with other values. Once you have done this, you can log in again wirelessly to your Gigaset SX541 WLAN dsl.

Configuring the Advanced Settings

In the ***Advanced Settings*** menu, you can configure all the options for the Gigaset SX541 WLAN dsl. If you want, you can also make changes to the settings you made using the wizard. The following table shows the options in the menu.

Menu	Description
Internet	This menu comprises all the setting options relating to the Internet. In particular, you can ◆ check and change the configuration for Internet access (see page 70) or specify a preferred DNS server (see page 74), ◆ set up Traffic Control for your Internet access (see page 76), ◆ configure the firewall, i.e. a number of security and special functions, for example access control for local PCs to the Internet or blocking certain Internet sites (see page 78), ◆ make the NAT settings needed to provide your own services on the Internet (see page 85), ◆ set up dynamic DNS for a static Internet address on your device (see page 90), ◆ configure the Quality of Service (see page 92).
Local Network	You can change the Private IP address of the Gigaset SX541 WLAN dsl here and make settings on the DHCP server (see page 93).
Wireless Network	You can configure the options here for wireless communication (SSID and encryption) and restrict access to the Gigaset SX541 WLAN dsl (see page 69).
Telephony	You can make the settings here for Internet telephony (VoiP) and you can configure you extensions (see page 104).
USB	You can make the settings here for operating an external data carrier, a Web server, a file server or a printer server on the USB port (see page 111).
Administration	You can make or change various system settings here, for example assign a password (see page 120), set the time (see page 119), or activate remote management (see page 121). You can also back up the data on your Gigaset SX541 WLAN dsl or load new firmware (see page 123).

Internet

If you have configured your Gigaset SX541 WLAN dsl using the two wizards, you have also already configured the WAN connection (Internet access). You can check or change these settings in the ***Internet*** menu.

This menu also offers you a wide range of possibilities for security settings and limiting access to the Internet as well as for providing your own services on the Internet.

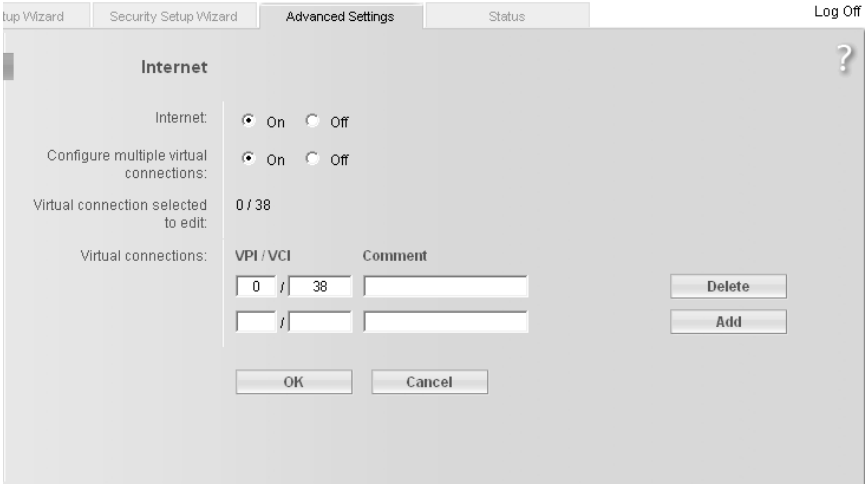
Via the ***Internet*** menu you can

- select or deselect the Internet connection and edit the virtual connection parameters (see below),
- check and edit the Internet configuration of the Gigaset SX541 WLAN dsl (see below),
- enter the PC's registered MAC address for Internet access (WAN interface) (for cloning the MAC address, see page 75),
- make DNS server settings (page 74),
- configure time and volume control for using the Internet (see page 76),
- protect your network against unauthorised access from outside (firewall) and limit or block access to Internet sites (see page 78),
- provide your own services on the Internet (NAT, see page 85),
- set up dynamic DNS (see page 90),
- define QoS properties (priorities for data transfer) (see page 92).

Internet Selection

On this screen you can select or deselect the Internet connection for your Gigaset SX541 WLAN dsl and edit the virtual connection parameters.

➔ Select ***Internet*** in the ***Advanced Settings*** menu.



➔ Select the appropriate option to select or deselect the Internet function of the Gigaset SX541 WLAN dsl.

You can edit the displayed virtual connection or add a new connection.

➔ Enter the new parameters in the ***VPI / VCI*** fields.

➔ Click ***Select*** to select the virtual connection for use.

➔ Click ***Delete*** to delete an entry.

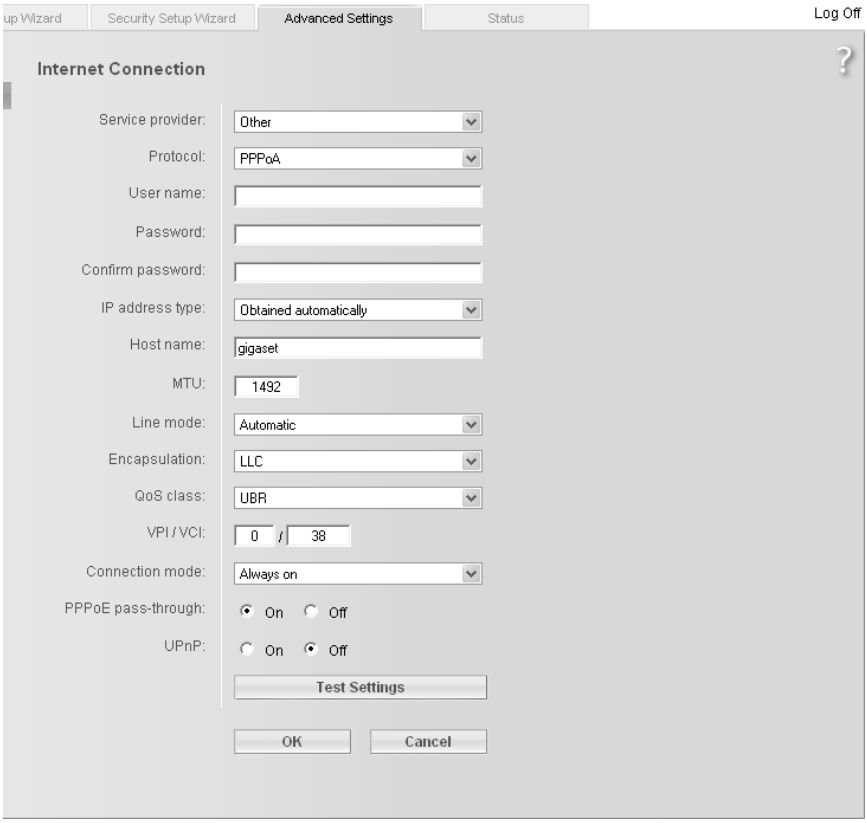
➔ Click ***Add*** to create a new entry.

➔ Click ***OK*** to save and apply the changes.

Internet Connection

On this screen you can set up or change the configuration of your Internet connection. Any settings you make here must coincide with the features your Internet provider makes available to you. False information can lead to problems with your Internet connection.

➔ If you wish to set up or change the settings for the Internet connection, select ***Internet Connection*** in the ***Advanced Settings*** – ***Internet*** menu.



➔ Select ***Other*** from the ***Service provider*** selection menu.

➔ Enter the data you have been given by your Internet provider: ***Protocol***, ***User name*** and ***Password***.

Leave the default settings for the parameters ***IP address type***, ***Host name***, ***MTU***, ***Line mode***, ***Encapsulation***, ***QoS class*** and ***VPI / VCI*** unless you have been given other data by your service provider.

Please remember:
To configure the Internet connection successfully, all fields must be filled in with the precise details given by your provider.

➔ Select how Internet sessions are to be established via ***Connection mode***:

– Select ***Always on*** if the connection is to exist at all times when the Gigaset SX541 WLAN dsl is switched on.

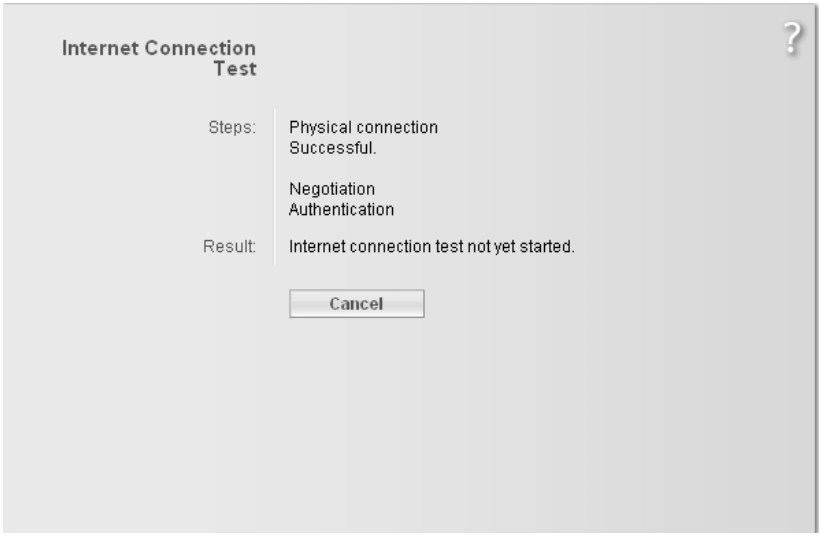
Please remember:
If you have a time-based tariff, this option can result in high connection charges.

– Select ***Connect on demand*** if applications such as a Web browser or an e-mail program are to connect to the Internet automatically.
– In the ***Idle time before disconnect*** field, enter a period of time after which the Internet connection is to be automatically ended if no data is transmitted (default setting: 3 minutes).

  You can deactivate this function by entering "0". This means that the connection will continue to exist even if no data is transmitted. If you have a time-based tariff, this can result in high charges. In this case you should enter a value other than "0".

  This time setting only applies to the ***Connect on demand*** option.
– Select ***Connect manually*** if you always want to establish and end the connection to the Internet manually. If you have a time-based tariff this will save you high connection charges. How to establish a connection manually is described on page 118.

➡ Click ***Test Settings*** to check the Internet connection. The router will attempt to connect to the Internet. Any Internet connection already in existence will be closed first.



You will then be returned to the ***Internet Connection*** screen. If necessary, you can now amend your entries.

➡ If the test was successful, click ***OK*** to apply the settings.

PPPoE pass-through

If you activate the ***PPPoE pass-through*** function, a PC in the network can connect to the Internet via its own connection ID. The router puts these connections through.

➡ In the ***Advanced Settings*** – ***Internet*** menu, select ***Internet Connection***.

➡ Select the option ***On*** to activate ***PPPoE pass-through***.

➡ Click ***OK*** to apply the settings.

Using UPnP (Universal Plug and Play)

PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered on the network.

Please remember:

The PC must have Windows ME or Windows XP as its operating system. Check whether the UPnP function has been installed in your PC's operating system. It may be necessary to retrospectively install the UPnP components even on Windows XP or Windows ME systems. Please consult your PC's operating instructions.

As soon as you have installed UPnP in the operating system of a PC and activated it on the router, applications on this PC (for example Microsoft Messenger) can communicate via the Internet without your needing to expressly authorise it. In this case, the router automatically implements port forwarding (Port Forwarding, see page 88), thereby facilitating communication via the Internet.

You will see a symbol for your Gigaset SX541 WLAN dsl on the task bar on the PC on which UPnP is installed. Windows XP systems will also include the icon under network connections. Clicking on this icon opens the Gigaset SX541 WLAN dsl's configuration screens.

➔ In the ***Advanced Settings*** – ***Internet*** menu, select ***Internet Connection***.

➔ Select ***UPnP***.

Please remember:

When the UPnP function is active, system applications can assign and use Ports on a PC. This can be a security risk.

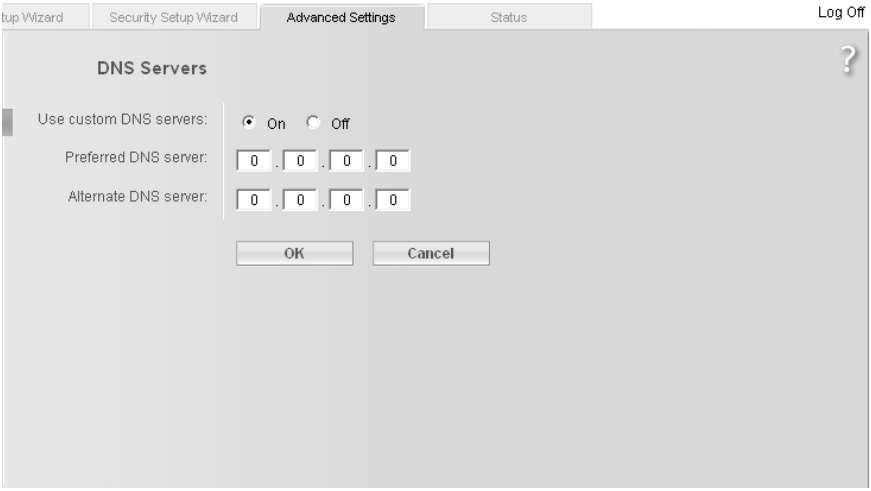
➔ Click ***OK*** to apply the settings.

DNS Server

DNS is a decentralised service which assigns PC names or Internet addresses (Domain names) and IP addresses to one another. A DNS server has to administer this information for each server or each LAN with an Internet connection.

Normally your Internet provider provides you with a DNS server, which makes this assignment when connection is set up to the Internet. If necessary, you can define the DNS server to be used for the Internet connections manually.

➔ In the ***Advanced Settings*** – ***Internet*** menu, select ***DNS Servers***.



➔ Activate the ***Use custom DNS servers*** function via the option ***On***.

➔ Enter the IP addresses for your preferred DNS servers (***Preferred DNS server*** and ***Alternate DNS server***).

➔ Click ***OK*** to apply the settings.

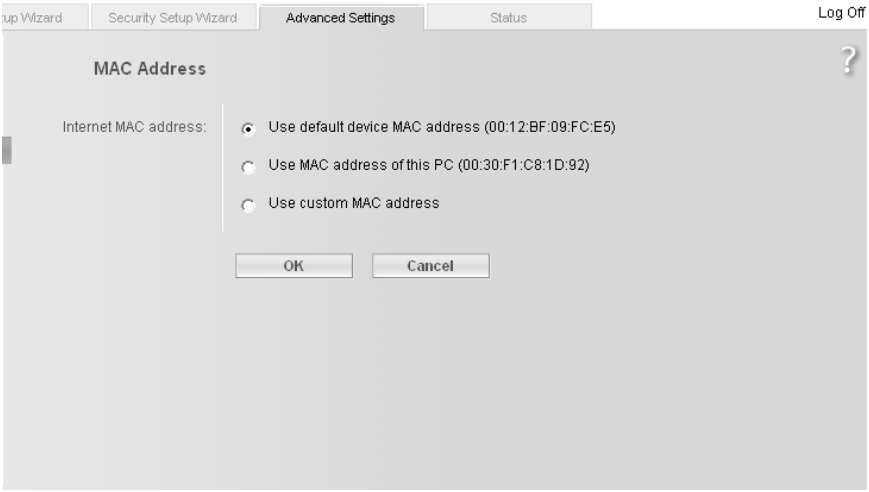
MAC Address

If you had Internet access through the same Internet provider before connecting the Gigaset SX541 WLAN dsl, then it is possible that the MAC address of one of your PCs has been used for registration when the connection was being set up. You must then either replace the current MAC address with the MAC address registered with the Internet provider or ask your Internet provider to register a new MAC address for your account.

Carry out the following steps:

➔ Connect a PC to the Gigaset SX541 WLAN dsl and open the configuration environment.

➔ In the ***Advanced Settings*** – ***Internet*** menu, select ***MAC Address***.



➔ Select which MAC address is to apply to the Internet connection:

- ***Use default device MAC address***: You can leave this default setting if the MAC address of the Gigaset SX541 WLAN dsl is used for connecting to the Internet.
- ***Use MAC address of this PC***: Select this option if the MAC address of the currently connected PC has previously been registered for connecting to the Internet or if you have re-registered the MAC address of the PC on which you are currently working.
- ***Use custom MAC address***: Select this option if you have asked your Internet provider to register a new MAC address and this is not the MAC address of the PC on which you are currently carrying out the configuration.

➔ Click ***OK*** to apply the settings.

Traffic Control

Traffic control allows you to control monthly Internet usage in terms of online time and transmitted data volume. You can specify general limits for your local network and individual ones for individual PCs.

Note:
Traffic control is only possible if the Internet connection is established directly through the Gigaset SX541 WLAN dsl and not via a PC or a different router.

➔ In the ***Advanced Settings*** – ***Internet*** menu, select ***Traffic Control***.

➔ If you want to monitor and limit monthly Internet usage within your network, select the option ***On*** for ***Traffic Control.***

➔ In the ***Reset traffic counters*** field, enter the day of the month on which the counters for the time and volume are automatically reset. Ask your Internet provider about the relevant billing day.

➔ Activate the option ***Automatically disconnect from the Internet*** if the Internet connection is no longer to be available when a time or volume limit is exceeded.

Global time limit

➔ Activate or deactivate the time limit available to all users in your network for surfing the Internet each month. This makes sense if your Internet tariff is time-based.

➔ Enter the total amount of time available per month in hours.

Global volume limit

➔ Activate or deactivate the limit on the data volume available to all users in your network for surfing the Internet (download and upload) each month. This makes sense if your Internet tariff is volume-based.

➔ Enter the total volume of data available per month in megabytes (MB).

Individual limits

You can specify individual limits for data volumes for individual PCs within your network.

➔ Select or deselect ***Individual limits***.

➔ Enter the MAC address of the PC and a device name for identification.

➔ In the ***Volume limit*** field, enter the data volume available per month in megabytes (MB). A standard volume limit is used for all non-listed clients.

➔ Click ***Delete*** to delete an entry.

➔ Click ***Add*** to create a new entry with the entered data or for the selected PC.

➔ Click ***OK*** to save and apply the changes.

You can check at any time how much time and volume are still available this month in the ***Status*** – ***Traffic Control*** menu (see page 133) and on the login screen for the configuration program under ***Traffic Control*** (see page 48).

Please remember:

The values recorded by your device for online time and transmitted data volume are only intended for your guidance and may differ from the exact values determined by your Internet provider.

Firewall

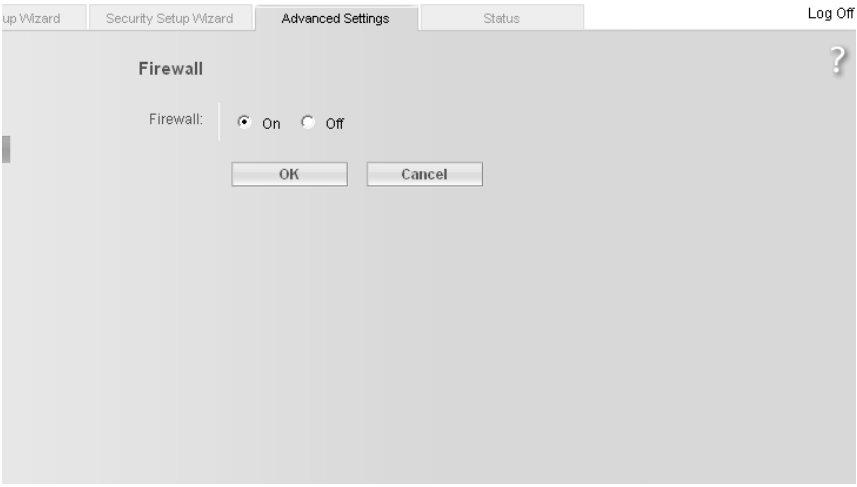
The firewall functions of the Gigaset SX541 WLAN dsl include various security functions for your local network.

You can:

- protect your network against hacker attacks (see below),
- block individual PCs' access to selected services or Internet sites (see page 81) or restrict them by means of a schedule rule (see page 84).

The firewall functions for Gigaset SX541 WLAN dsl are activated and configured in the factory. If you wish to deactivate the firewall, carry out the following steps:

➔ In the ***Advanced Settings*** – ***Internet*** menu, select ***Firewall***.



➔ Select the required option.

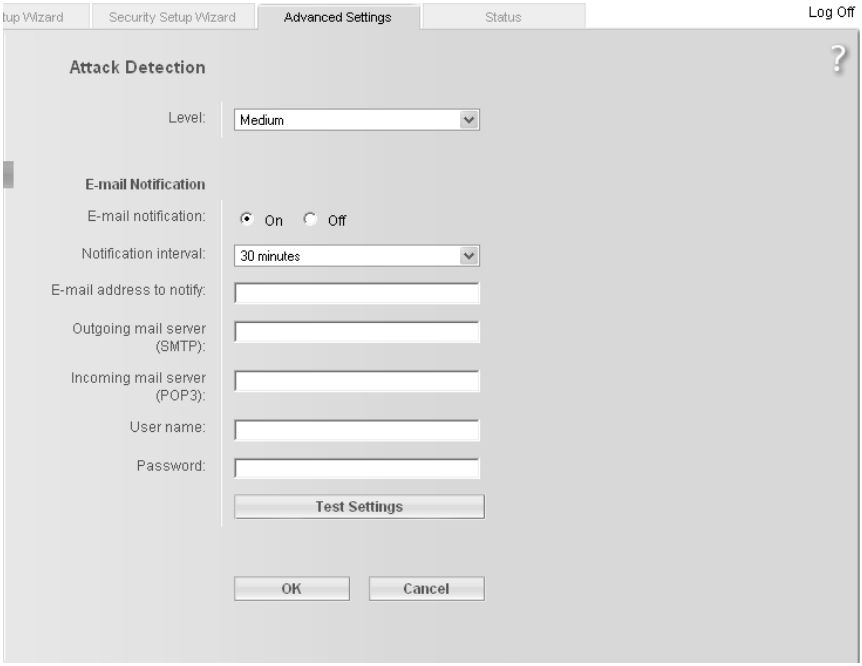
➔ Click ***OK*** to apply the settings.

Attack Detection

If the firewall functions of your Gigaset SX541 WLAN dsl are activated, the device monitors and limits the access of incoming traffic via the DSL connection with a function called Stateful Packet Inspection (SPI). This allows the Gigaset SX541 WLAN dsl to identify and prevent certain types of attack from the Internet, such as Denial-of-Service (DoS). DoS attacks are aimed at devices and networks with Internet connections. The aim is not so much to steal data but to paralyse the computer or network to such an extent that the network resources are no longer available. A typical hacker attack involves making a remote computer announce that it is acting for the paralysed device, for example, and receive the data meant for it.

You can use the Attack Detection function to change the standard firewall settings and arrange to be notified by email about any attempted hacker attacks.

➔ In the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu, select ***Attack Detection***.



➔ Select the security level for the firewall:

- The default level ***Medium*** offers you high security with scarcely limited functionality for special applications.
- The level ***High*** offers you maximum security with possibly limited functionality for special applications.
- The level ***Low*** offers you maximum functionality with possibly reduced security.
- Select ***Custom*** to determine the criteria for defence against hacker attacks yourself. Further setting options are then shown in the window (see page 80).

E-mail notification of a hacker attack

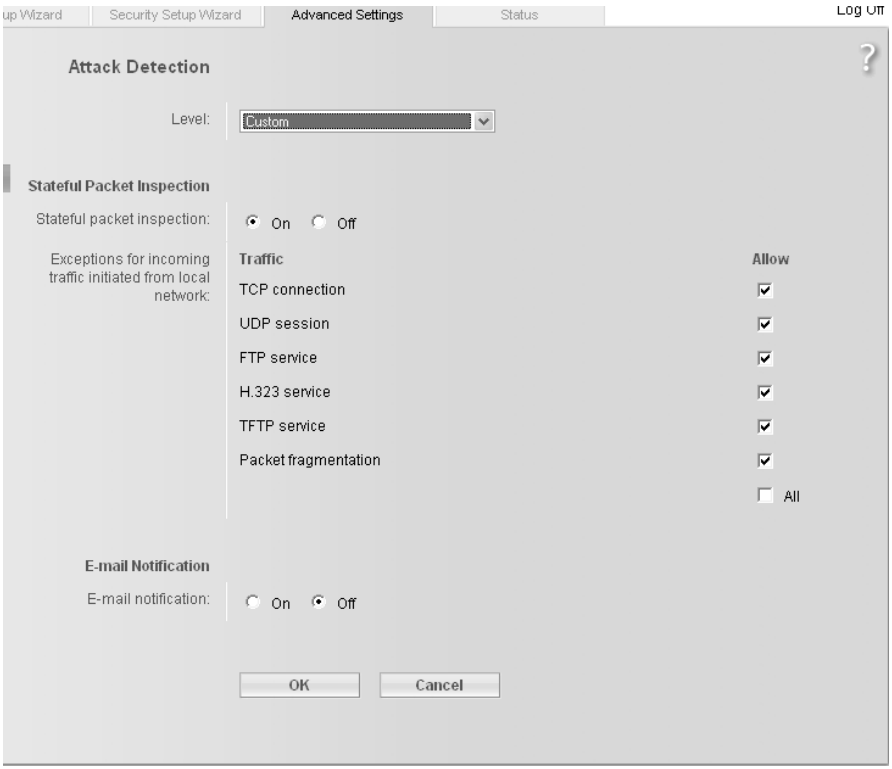
You can choose to be informed by e-mail about a possible hacker attack.

➔ Enter the following in the dialogue fields:

- Select the ***Notification interval***, i.e. at what intervals you wish to be informed about hacker attacks. If hacker attacks have been identified and blocked in the intervening period, you will receive a summary about each event.
- ***E-mail address to notify***: Enter the e-mail address to which the notifications are to be sent.
- ***Outgoing mail server (SMTP)***: Enter the address of the outgoing mail server through which your device can send you the notifications.
- ***Incoming mail server (POP3)***: If your outgoing mail server demands authentication via POP3 before e-mails can be sent, enter the address of the outgoing mail server here.
- Enter your ***User name*** and the relevant ***Password***.

➔ Click ***Test Settings*** to check the details for the e-mail notification.

User-defined settings



- Stateful Packet Inspection

  Your device monitors and limits the access of incoming traffic from the Internet with SPI (Stateful Packet Inspection). This allows it to identify and block certain types of attack such as Denial-of-Service (DoS). A typical DoS attack involves a remote computer paralysing a system and announcing that it is acting for the paralysed device in order to receive the data meant for it. For the level ***Custom*** you can specify yourself whether you wish to activate SPI on your device and which exceptions you wish to make.

➔ Activate or deactivate ***Stateful Packet Inspection*** for your device's Internet connection.

➔ Select the services for which you also wish to allow incoming ***Traffic*** if it has been initiated by a client in your LAN. If you select the ***All*** option at the end of the list you can permit all services.

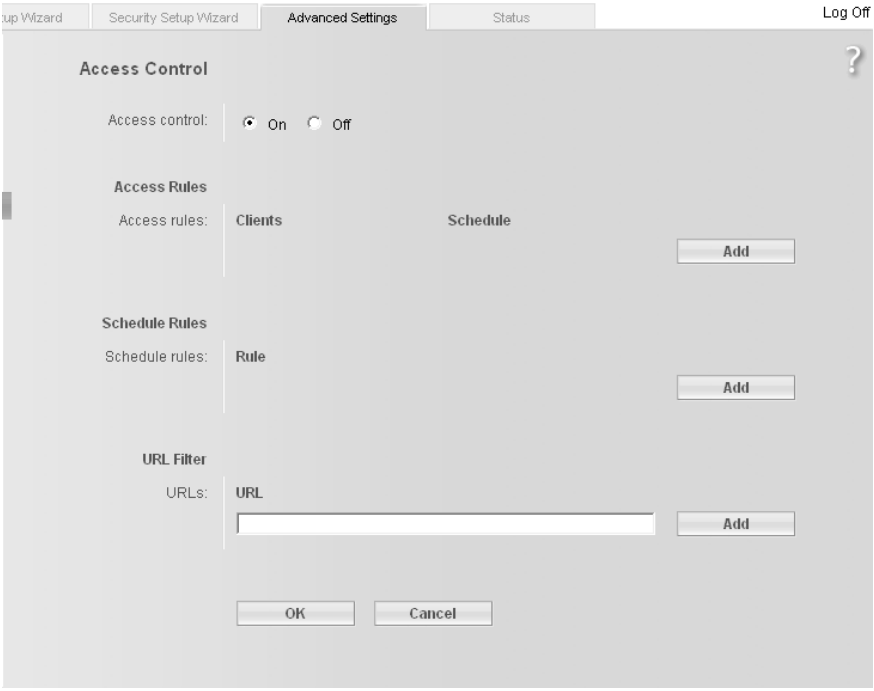
➔ Click ***OK*** to apply the settings.

Setting up Access Control to the Internet

The ***Access Control*** function allows you to block access to various Internet services for one or more PCs. You can limit these blocks to certain days and hours with ***Schedule Rules***.

➔ Select ***Access Control*** in the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu.

➔ Activate the ***Access Control*** function via the option ***On***.



You have the following setting options for ***Access Control***:

URL filter

The URL filter allows you to block access to certain Internet sites or Internet domains. Once you have entered the relevant URLs, you can then create access rules that apply the URL filter for the selected clients in your network.

➔ Enter the required URL in the field.

➔ Click ***Add*** to create a new entry.

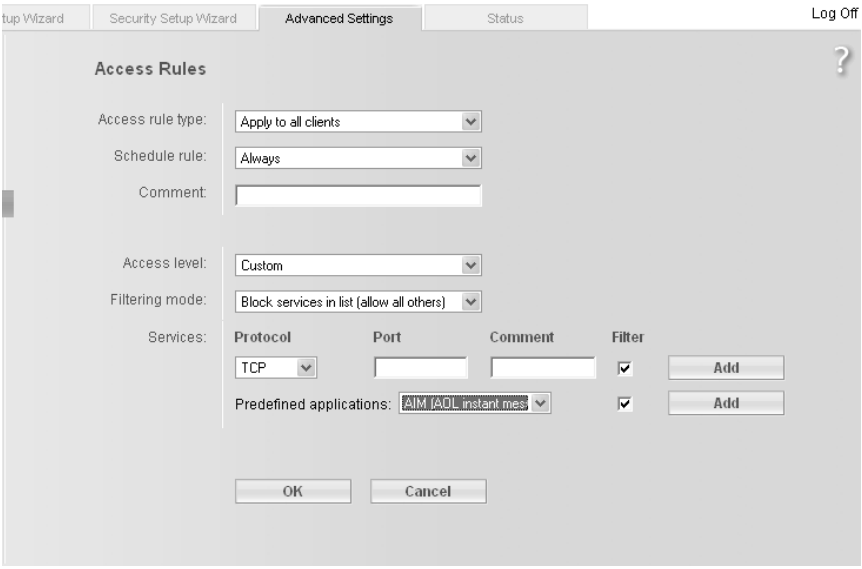
➔ Click ***Delete*** to delete an entry.

➔ Click ***OK*** to apply the settings.

Access Rules

You can limit access to the Internet for all or for certain clients in your local network. You can assign a ***Schedule rule*** to each access rule and allow or block access to URLs and services.

➔ Click ***Add*** to create an access rule.



➔ Select the ***Access rule type*** from the list:

- ***Apply to all clients***: The rule applies to all PCs in your network.
- ***Specify IP address range***: You select the PCs to which the rule is to apply by entering an IP address block.
- ***Specify IP address*** or ***Specify MAC address***: The rule applies to a PC you select via the IP address or MAC address.

➔ Select a ***Schedule rule***: The default setting is ***Always***. You can create more ***Schedule Rules*** in the ***Access Control*** field (see page 84).

➔ Enter a name for the ***Comment*** for the access rule.

➔ Define the ***Access level***.
You can apply ***Deny access to the Internet***, ***Allow web browsing with URL filter***, ***Allow web browsing*** or make user-defined settings:

- Select whether the URL filters you have set (see page 82) are to be activated.
- If you wish to create a ***Service filter***, activate this option.
- In ***Filtering mode***, determine whether the services you select are to be allowed or blocked.
- Select the ***Services*** you wish to allow or block.

  Select the ***Protocol*** and enter the appropriate ***Port*** (a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example **80,90–140,180**). The ***Description*** displayed helps you to identify different services.
- Activate the ***Filter*** option to use the relevant service for the service filter.
- You can also select services from the ***Predefined applications*** list.

– Click ***Delete*** to delete an entry. Click ***Add*** to create a new entry with the entered data or for the selected, predefined application.

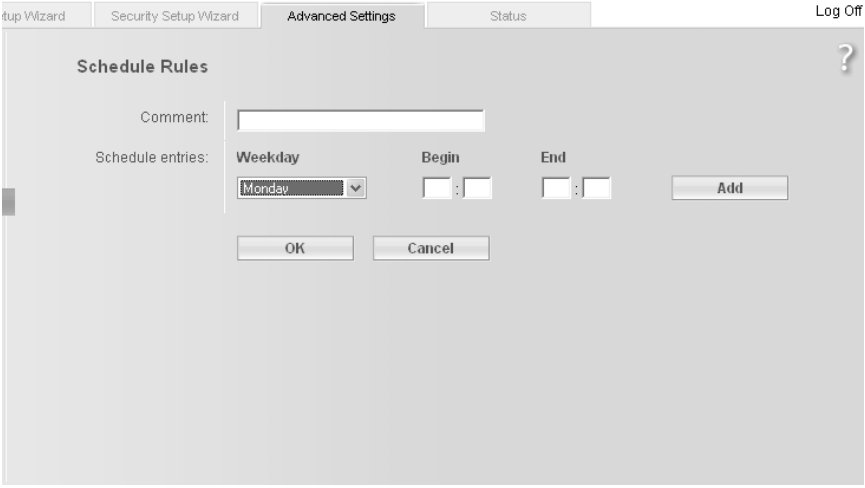
➔ Click ***OK*** to apply the settings.

Schedule Rules

If you have set up an access rule (see page 82) for certain services in the Internet, you can control it by means of a schedule rule. A schedule rule determines the period of time for which a defined access control is active.

You can define several rules. A rule takes effect when you select ***Access Rules*** in the menu and activate it.

➔ In the ***Access Control*** field under ***Schedule Rules***, click ***Add***.



➔ Assign a name to the new rule under ***Comment***. This name will then appear in the selection list on the screen for the menu entry ***Access Rules***.

➔ Select the day of the week from the list or else the option ***Every day***.

➔ Enter the time for the rule to ***Begin*** and ***End***.

➔ Click ***Add*** to define a new rule.

➔ Click ***OK*** to apply the settings.

Setting up the NAT Function

Your Gigaset SX541 WLAN dsl comes provided with the NAT (Network Address Translation) function. With Address Mapping, several users in your local network can access the Internet via one or more public IP addresses. In the default setting, all the local IP address are mapped to your router's public IP address.

One of the characteristics of NAT is that data from the Internet is not allowed into your local network unless it has been explicitly requested by one of the PCs in that network. Most Internet applications run behind the NAT firewall without any problems. If you request Internet pages, for example, or send and receive e-mails, the request for data from the Internet comes from a PC in the local network and so the router allows the data through. The router opens exactly **one** port for the application. A port is an internal PC address through which the data is exchanged between a server on the Internet and a client on a PC in the local network. Communicating via a port follows the rules of a particular protocol (TCP or UDP).

If an external application tries to send a call to a PC within the local network, the router will block it. There is no open port via which the data could enter the local network.

Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to the user in the local network. These applications cannot work if Network Address Translation (NAT) has been activated.

Using port forwarding (the forwarding of requests to particular ports) the router is forced to forward requests from the Internet for a certain service, fro example a game, to the appropriate port or ports on the PC on which the game is running.

Port triggering is a specific variant of port forwarding. Unlike port forwarding, in this case the Gigaset SX541 WLAN dsl forwards data from the set port block to the PC that has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in your network, rather to the port numbers of the required Internet service.

Where configuration is concerned, this means:

- You have to define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that have to be opened for the application to this trigger port.
- The router checks all outgoing data for the port number and protocol. If it recognises a match of port and protocol to a defined trigger port, it will open the assigned public ports and note the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, it allows the data through and directs it to the right PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, it is simply ignored by the router.

Please remember:

- An application that is configured for port triggering can only be run by one user in the local network at a time.
- As long as the public ports are open, they can be used by unauthorised persons to gain access to a PC in the local network.

When the Gigaset SX541 WLAN dsl is supplied, the NAT function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet.

You can use the NAT settings for the Gigaset SX541 WLAN dsl to

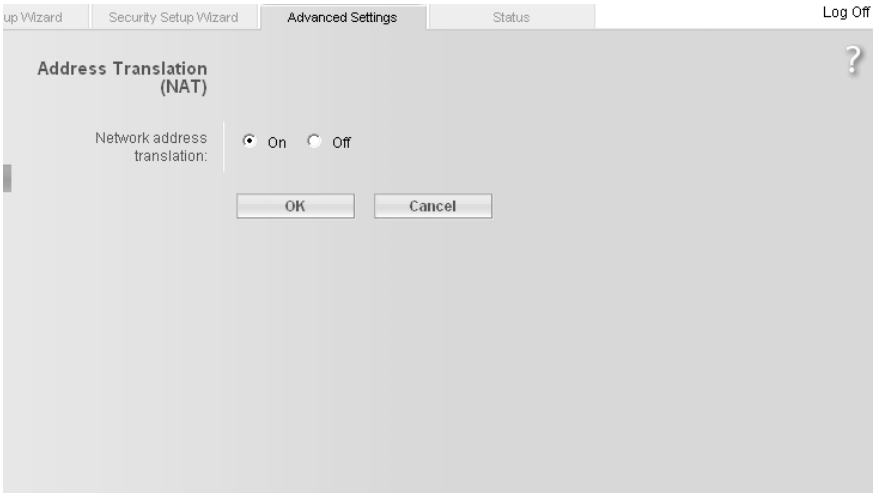
- set up port triggering for special applications (see page 87),
- set up the Gigaset SX541 WLAN dsl as a virtual server by configuring Port Forwarding (see page 88),
- open the firewall for selected PCs (see page 89).

Please remember:

You must make sure for the functions described below that the IP addresses of the PCs do not change. If the IP addresses of the PCs are assigned via the DHCP server of the Gigaset SX541 WLAN dsl, you must select the option ***Never expires*** (see page 94) for the settings on the ***Local Network*** screen for ***Lease time*** or assign static IP addresses for the PCs.

You can activate or deactivate the NAT function (default setting: NAT function is activated).

➔ In the ***Advanced Settings*** – ***Internet*** menu, select ***Address Translation (NAT)*** and select the required option.

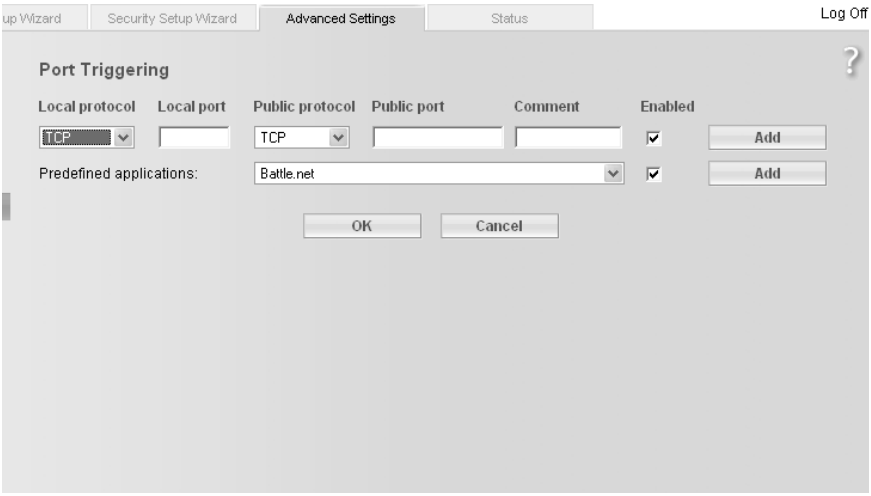


Port Triggering

If you configure port triggering for a certain application, you need to identify a so-called trigger port and the protocol (TCP or UDP) this port uses. You then assign the public ports that have to be opened for the application to this trigger port.

You can select known Internet services for this or assign ports or blocks of ports manually.

➔ To set up port triggering for a service, select ***Port Triggering*** in the ***Address Translation (NAT)*** menu.



➔ Select the required application from the ***Predefined applications*** list.

➔ Select the option in the ***Enabled*** column.

➔ Click the ***Add*** button. The data for the required service is entered on the screen.

If the application you require is not in the list, you must enter the relevant data on the screen manually:

➔ ***Local protocol***: Select the protocol that is to be monitored for outgoing traffic.

➔ ***Local port***: Enter the port that is to be monitored for outgoing traffic.

➔ ***Public protocol***: Select the protocol that is to be allowed for incoming data traffic.

➔ ***Public port***: Enter the port that is to be opened for incoming traffic.

> **Note:**
> You can enter a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a dash or any combination of these, for example **`80,90-140,180`**).

➔ ***Comment***: Enter a description to help you identify different entries.

➔ Select the option in the ***Enabled*** column.

➔ Click the ***Delete*** button to delete an entry. Click the ***Add*** button to add a new entry.

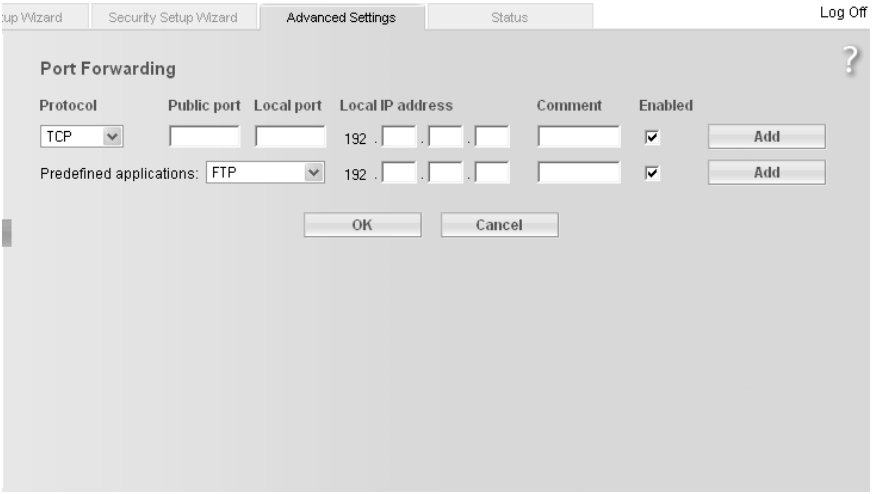
➔ Apply the settings by clicking ***OK***.

Port Forwarding

If you configure Port Forwarding, the Gigaset SX541 WLAN dsl outwardly assumes the role of the servers. It receives requests from remote users under its public IP address and automatically redirects them to local PCs. The private IP addresses of the servers in the local network remain protected.

Internet services are addressed via defined port numbers. The Gigaset SX541 WLAN dsl needs a mapping table of the port numbers to redirect the service requests to the server that actually provides the service. Port Forwarding has to be configured for this purpose.

➔ To set up port forwarding for a service, select ***Port Forwarding*** in the ***Address Translation (NAT)*** menu.



➔ Select the required application from the ***Predefined applications*** list.

➔ Select the option in the ***Enabled*** column.

➔ Click the ***Add*** button. The data for the required service is entered on the screen.

If the application you require is not in the list, you have to enter the relevant data on the screen manually:

➔ Select the protocol for the service you are providing from the ***Protocol*** list.

➔ Under ***Public port,*** enter the port number of the service you are providing.

➔ In the ***Local port*** field, enter the internal port number to which service requests are to be forwarded.

➔ In the ***Local IP address*** field, enter the IP address of the PC that provides the service.

Example: the Web server has been configured to react to requests on port 8080. However, the requests from ripostes enter by port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with the port number 80 on the Web server of the PC you have defined with port 8080.

Note:
You can enter a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, e.g. **80,90–140,180**).

➔ ***Comment***: Enter a description to help you identify different entries.

➔ Select the option in the ***Enabled*** column.

➔ Click ***Add***.

➔ Click ***Delete*** if you wish to delete the data in the relevant line again.

➔ Click ***OK*** to apply the settings.

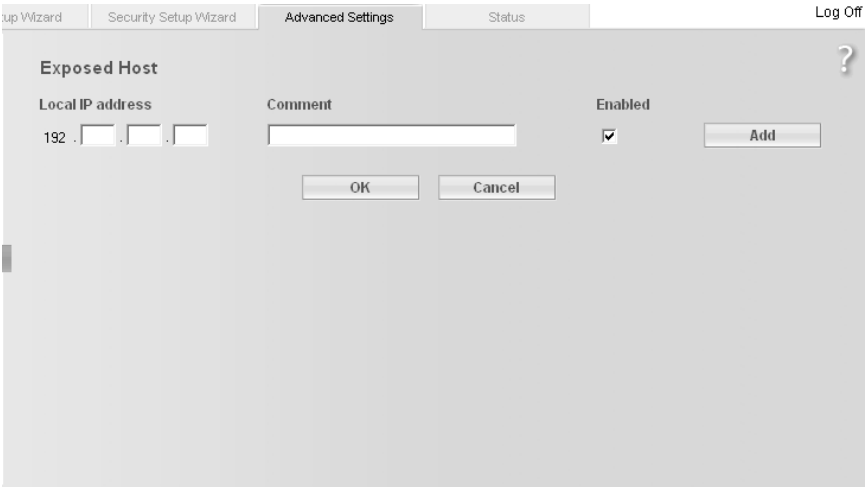
Opening the Firewall for Selected PCs (Exposed Host)

You can set up a client in your local network to be an exposed host. Your device will them forward all incoming data traffic from the Internet to this client. You can then, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users.

As the exposed host, your local client is directly visible to the Internet and therefore particularly exposed to risk (for example from hacker attacks). You should only activate this function if it is absolutely necessary (for example to operate a Web server) and other functions (for example port forwarding) are not adequate. In this case you should take appropriate measures on the clients concerned.

Please remember:
Only one PC per public IP address can be set up an Exposed Host (see also Section "Port Forwarding" on page 88.

➔ To set up a PC an exposed host, select ***Exposed Host*** in the ***Address Translation (NAT)*** menu.



➔ Enter the ***Local IP address*** of the PC that is to be enabled an Exposed Host.

➔ Enter a name for the PC in the ***Comment*** field.

➔ Activate the entry ***Enabled*** by selecting the option.

➔ Click the ***Add*** button to add the entry to the list.

➔ Click the ***Delete*** button to delete the entry from the list.

➔ Apply the settings by clicking ***OK***.

Dynamic DNS

Any service you provide on the Internet can be accessed by a Domain names. Your router's Public IP address is assigned to this domain name. If your Internet Service Provider for your local network's WAN connection assigns the IP address dynamically, the IP address of the router can change. The assignment to the domain name will no longer be valid and your service will no longer be available.

In this case, you must ensure that the assignment of the IP address to the domain name is updated regularly. This is handled by the dynamic DNS service (DynDNS). You can use the DynDNS service to assign your Gigaset SX541 WLAN dsl an individual static domain name on the Internet even if it does not have a static IP address.

There are various providers on the Internet offering a free DynDNS service.
The Gigaset SX541 WLAN dsl uses the DynDNS service from **DynDNS.org** (http://www.DynDNS.org). If you use the service of this DynDNS provider, your service can be reached on the Internet as a subdomain of one of the DynDNS.org domains.

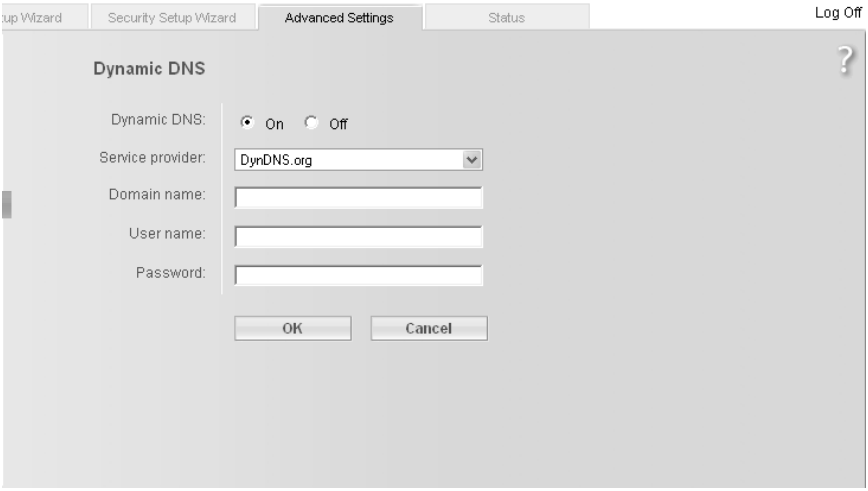
If you have activated the device's DynDNS function, it will monitor its public IP address. When this changes, it will open a connection to DynDNS.org and update its IP address there.

Please remember:

You have to open an account with DynDNS.org before you can use the Gigaset SX541 WLAN dsl's DynDNS function. Follow the instructions on the DynDNS.org. weepiest. Then enter the user data when configuring the router.

➔ To use the router's DynDNS function, select ***Dynamic DNS*** in the ***Advanced Settings*** – ***Internet*** menu.

➔ Activate the ***Dynamic DNS*** function.



➔ From the ***Service provider*** list, select the service offering dynamic DNS (DynDNS.org or TZO.com).

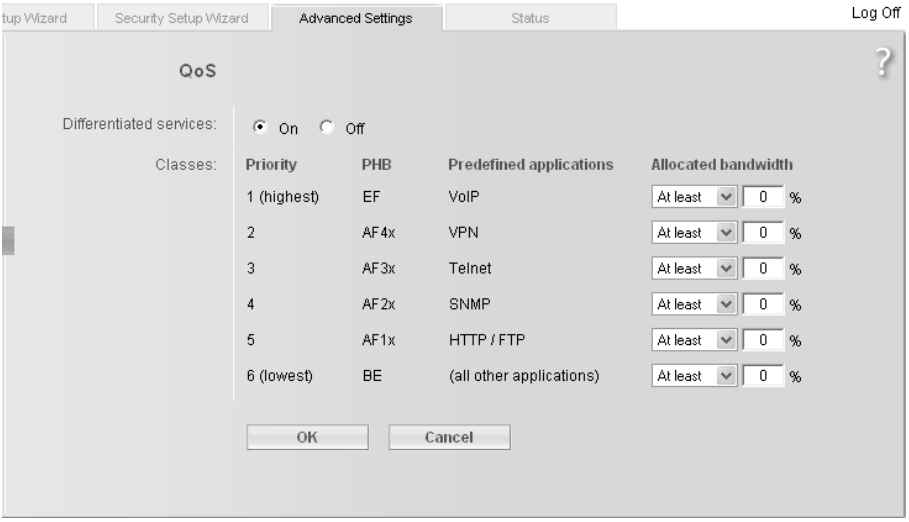
➔ Enter ***Domain name***, ***User name*** and ***Password***. You will have received the necessary information when registering with your ***Service provider***.

➔ Click ***OK*** to apply the settings.

QoS (Quality of Service)

Many communication and multimedia applications require high speed and large bandwidths to transfer data between the local network and the Internet. However, for many applications there is often only one Internet connection available with limited capacity. ***QoS*** (Quality of Service) divides this capacity between the different applications and provides undelayed, continuous data transfer where data packets with higher priority are given transmission preference.

➔ In the ***Advanced Settings*** – ***Internet*** menu, select the entry ***QoS***.



➔ Select ***Differentiated services***, i.e. the priorisation of certain services for data transfer between your network and the Internet.

You can determine via ***Priority*** which data packets are to be given preferential transmission. With the aid of ***PHB*** (Per Hop Behaviours) a decision is also made about whether data packets are to be forwarded immediately before all others (***EF***, Expedited Forwarding), guaranteed and without data loss (***AF***, Assured Forwarding) or normally (***BE***, Best Effort). If your application already supports QoS, your application will determine the priority automatically and this will be noted by your device for forwarding. In addition, your device recognises certain ***Predefined applications*** and gives each data packet the relevant priority. You can also determine which proportion of the bandwidth for your Internet connection is to be made available for a certain class as ***Allocated bandwidth***.

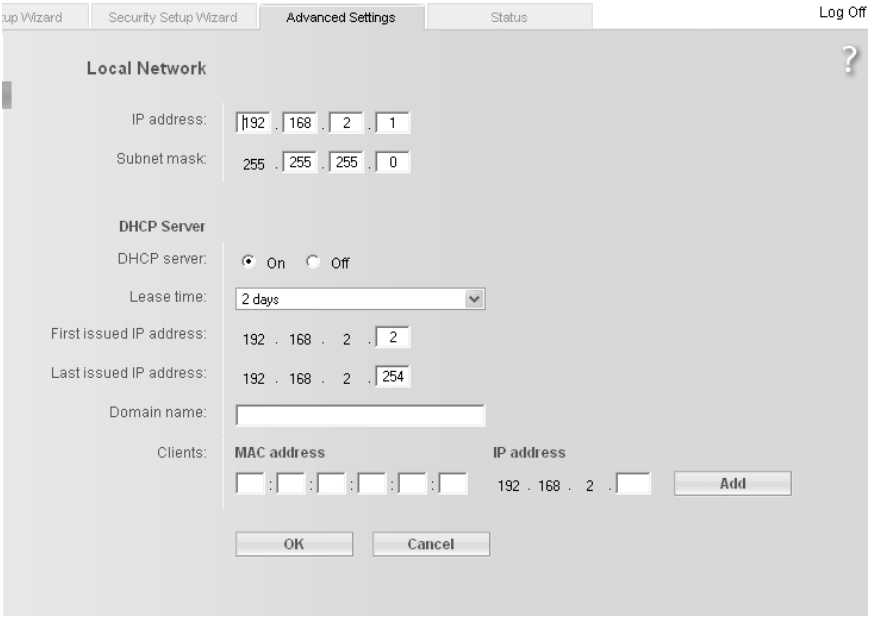
➔ Select the ***Allocated bandwidth*** for the ***Predefined applications*** and for the line ***(all other applications)***.

➔ Click ***OK*** to save and apply the changes.

LAN Configuration

You can use the LAN configuration to define an IP address for the Gigaset SX541 WLAN dsl and configure the DHCP server.

➔ Select ***Advanced Settings*** – ***Local Network***.



Defining the private IP address for the Gigaset SX541 WLAN dsl

You can change the device's IP address on this screen. The preset IP address is 192.168.2.1. This is the Private IP address of the Gigaset SX541 WLAN dsl. This is the address under which the device can be reached in the local network. It can be freely assigned from the block of available addresses. The IP address under which the Gigaset SX541 WLAN dsl can be reached from outside is assigned by the Internet service provider.

➔ If you want to assign the Gigaset SX541 WLAN dsl a different IP address, enter it in the fields next to ***IP address***.

➔ Select a number from the ***Subnet mask*** list.

We recommend using an address from a block that is reserved for private use. This address block is 192.168.1.1 – 192.168.255.254.

Please remember:

New settings can only be made after rebooting the Gigaset SX541 WLAN dsl. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

Configuring the DHCP server

The Gigaset SX541 WLAN dsl has a DHCP Server for which the factory setting is active. As a result, the IP addresses of the PCs are automatically assigned by the Gigaset SX541 WLAN dsl.

Please remember:

- If the DHCP server for the Gigaset SX541 WLAN dsl is activated, you can configure the network setting on the PC so that the ***Obtain an IP address automatically*** option is set. To find out how to do this, please read Section "Configuring the Local Network" on page 21.
- If you deactivate the DHCP server, you will have to assign a static IP address for the PCs using the network settings.

➔ To activate the DHCP server, select ***On***.

➔ If the DHCP server is active, you can define a ***Lease time***. The Lease time determines the period for which the PCs keep the IP address assigned to them without changing them.

Please remember:

If you select the ***Never expires*** option, the IP addresses are never changed. You should select this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign these PCs static IP addresses.

➔ Define the range of IP addresses that the Gigaset SX541 WLAN dsl should use to automatically assign IP addresses to PCs. Define the ***First issued IP address*** and the ***Last issued IP address***.

➔ You can define the name of a domain (Windows workgroup) in the ***Domain name*** field.

Assigning Static IP Addresses to Individual PCs

Even if you have activated the DHCP server, you can still assign individual PCs a static IP address (for example if you are setting up these PCs for NAT functions).

➔ Enter the ***MAC address*** and the name of the PC in the ***Device name*** field.

➔ Enter the ***IP address*** you wish to assign to the PC in the field below.

➔ Click the ***Add*** button to add the entry to the list.

➔ Click the ***Delete*** button to delete the entry from the list.

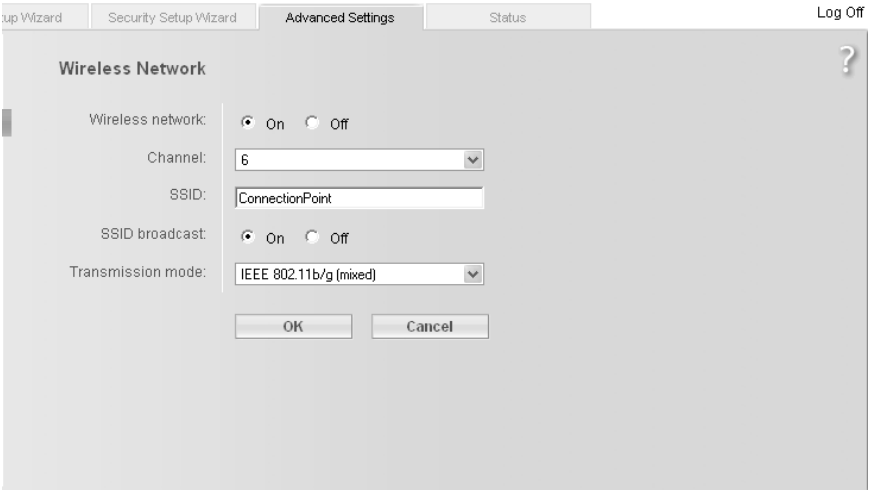
➔ Apply the settings by clicking ***OK***.

Configuring Wireless Connections

If PCs are communicating wirelessly via the Gigaset SX541 WLAN dsl, you should also take steps to enhance the security of your wireless network. You make this configuration via the ***Advanced Settings*** – ***Wireless Network*** menu. Here you can

- activate the Gigaset SX541 WLAN dsl's wireless module (see below),
- set the channel and SSID (see page 95),
- set Encryption for wireless transmissions (see page 97),
- restrict access to the Gigaset SX541 WLAN dsl's LAN (see page 97) and
- configure the repeater function on the Gigaset SX541 WLAN dsl.

➥ In the ***Advanced Settings*** menu, select ***Wireless Network***.



➥ Select the ***On*** option for ***Wireless Network*** (default setting).

Devices can only log in wirelessly if the Gigaset SX541 WLAN dsl's wireless module is activated.

You can now make the settings for your wireless network.

Channel

The set radio channel is used by all clients in your network for wireless data transfer. You can choose between various channels, depending on your current location.

➥ Select ***Automatic*** so that the best channel for transmitting the data is used automatically.

SSID

Before the wireless network components can communicate with each other, you must use the same SSID (Service Set Identifier).

The default SSID for the Gigaset SX541 WLAN dsl is **ConnectionPoint**. For security reasons you should change this SSID and deactivate SSID broadcast (see below).

Enter a character string of your choice. The SSID is case sensitive. It can be up to 32 alphanumerical characters long.

Please remember:
The connection to the wireless network adapters will be interrupted until you enter the new SSID on them as well.

SSID broadcast

If this option is enabled (default setting), the Gigaset SX541 WLAN dsl will send the SSID in all data transmissions and your Gigaset SX541 WLAN dsl's SSID will be displayed on PCs that have a wireless network adapter. In this case, eavesdroppers could use the SSID to gain access to your network.

If you deactivate ***SSID broadcast***, your Gigaset SX541 WLAN dsl's SSID will not be displayed. This increases the protection against unauthorised access to your wireless network. However, you must make a note of the SSID. You will need this to log on your PC.

➔ Select the ***Off*** option to deactivate ***SSID broadcast***.

Transmission mode

The IEEE 802.11g standard permits data transfer up to 54 Mbit/s and the IEEE 802.11b standard up to 11 Mbit/s. For the best possible data transfer rates in your network select ***IEEE 802.11g only***. To operate clients with older wireless network adapters in your network, select ***IEEE 802.11b/g (mixed)***.

➔ Select the required transmission mode for your wireless network.

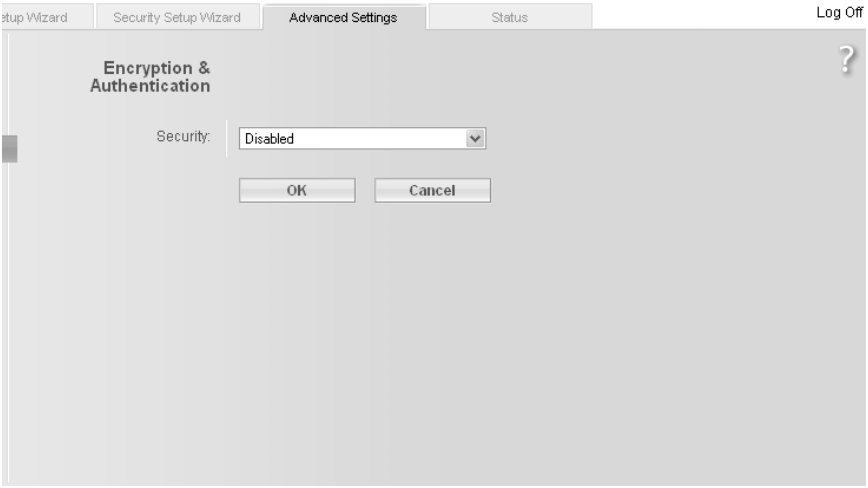
Setting Wireless Security

If you are sending data over wireless channels, we recommend that you activate encryption (WEP or WPA) on your wireless network components. WPA offers greater security than WEP. We therefore recommend that you choose WPA encryption if it is supported by all components in your wireless network.

WPA is a more advanced procedure than WEP for protecting wireless networks. Dynamic keys based on TKIP (Temporal Key Integration Protocol) offer increased security. The new WPA2 standard is based on AES.

WPA also supports the use of an authentication server.

➔ In the ***Wireless Network*** menu, select ***Encryption & Authentication***.



The following security mechanisms are currently available:

- WPA2-PSK and WPA2-PSK / WPA-PSK (see page 98)
- WAP2 and WPA2 / WPA with authentication server (see page 99)
- WEP encryption (Wired Equivalent Privacy) (see page 100)

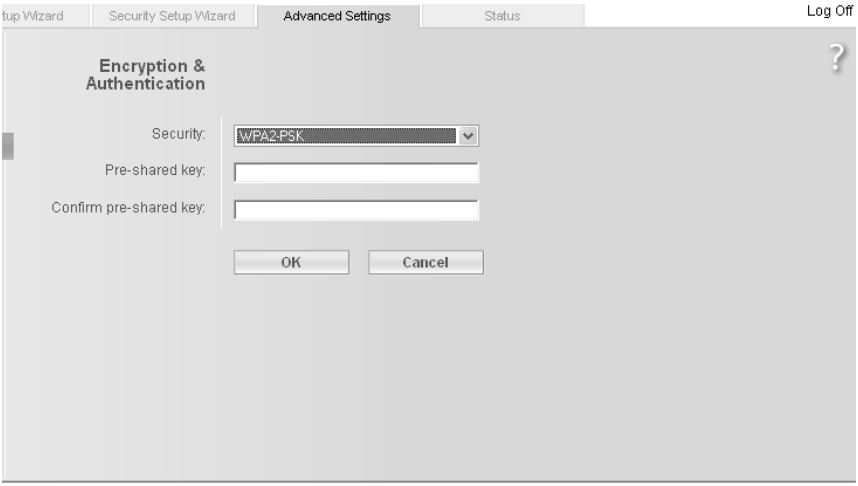
WPA2-PSK and WPA2-PSK / WPA-PSK

WPA with Pre-shared Key (WPA-PSK)

WPA-PSK is a special WPA mode that provides encryption protection for users at home and in small companies without a company authentication server. Encryption keys are automatically generated with the Pre-shared Key and automatically changed (rekeying) and authenticated between the devices after a certain period of time (Rekey Interval).

Which standard of encryption you can choose depends on the components in your wireless network. Every PC (network adapter) that requires access to a wireless network protected by WPA must also support WPA. To find out whether and how you can use WPA on your PC, read your network adapter's operating instructions. If all components support WPA2, select option ***WPA2-PSK***. If you are using network adapters that only support WPA, select the option ***WPA2-PSK / WPA-PSK***. The entries described below are the same for both options.

➔ Select the required option in the ***Security*** field.



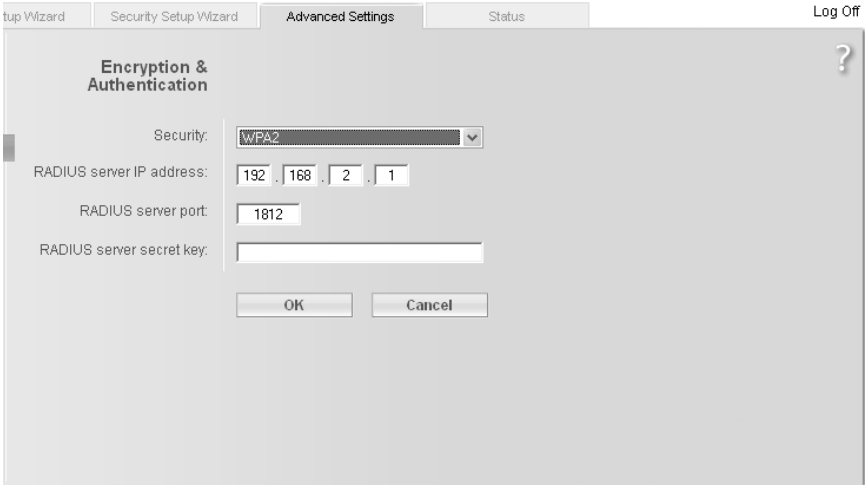
➔ Enter a key in the ***Pre-shared key*** field (up to 32 alphanumerical characters) and confirm it by entering it again.

➔ Apply the settings by clicking ***OK***.

WPA and WPA2 with authentication server

In large networks (for example in companies), WPA enables the use of an additional authentication service. In this case, user access is controlled by user accounts and passwords, in addition to WPA encryption. A RADIUS server acts as an authentication server. You can select the new ***WPA2*** standard if this is supported by all components in your wireless network, or select ***WPA2 / WPA*** if you are using devices that only support WPA.

➔ Select the required option in the ***Security*** field.



➔ Enter the IP address of the RADIUS server in the ***RADIUS server IP address*** field.

➔ Enter the port of the RADIUS server in the ***RADIUS server port*** field.

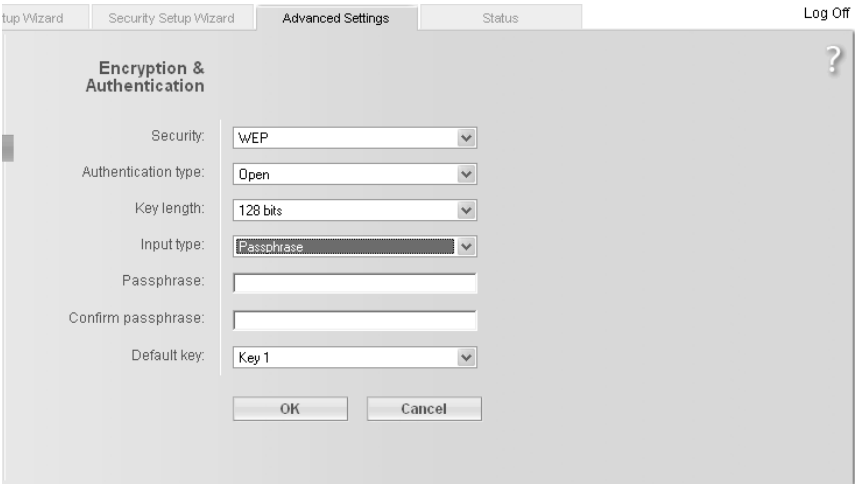
➔ In the ***RADIUS server secret key*** field, enter a keyword conforming to the conventions of the RADIUS server, which is to be used by the server for authentication.

➔ Click ***OK*** to apply the settings.

WEP Encryption

If WPA is not supported by all components in your wireless network, we recommend that you activate WEP Encryption on your wireless network components.

➔ In the ***Security*** field, select the option ***WEP***.



➔ Select the ***Authentication type***:

- Select ***Shared*** to require that each client logs in to the network with a specified key.
- Select ***Open*** to permit data transfer within your wireless network without the need for a key.

You can choose either the standard 64-bit key or the more robust 128-bit key for encryption. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for both the Gigaset SX541 WLAN dsl and all your wireless network adapters.

➔ Select the ***Key length***: 64 bits or 128 bits.

➔ Select the ***Input type***, i.e. whether you wish to enter the key manually or have it generated automatically by means of a ***Passphrase***.

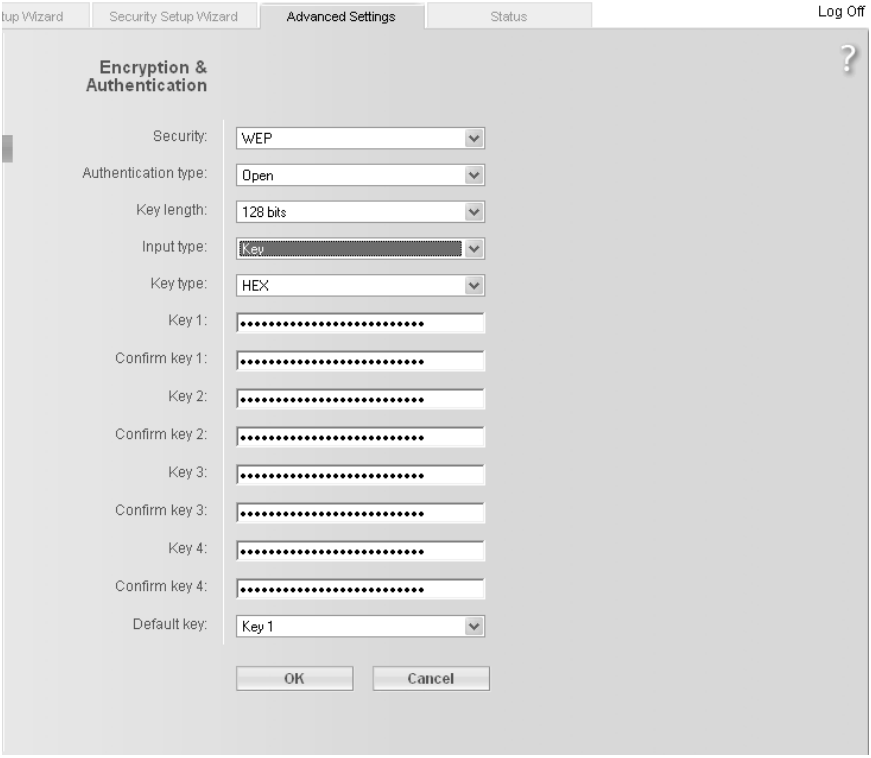
Generating the key by means of a Passphrase

➔ Enter a ***Passphrase*** (up to 32 characters) and confirm it by entering it again. Four keys are generated.

➔ Select one of the four keys as ***Default key***.

Manual key entry

➔ Select the ***Key type***, ***Hex*** or ***ASCII***.



If you select ***Hex,*** you can use the characters **0** to **9** and **A** to **F**.

– With a 64-bit encryption depth, the key is exactly 10 characters long.

  An example of a valid key: 1234567ABC

– With a 128-bit encryption depth, the key is exactly 26 characters long.
  An example of a valid key: 234567ABC8912345DEF1234567

If you select ***ASCII,*** you can use the characters **0** to **9**, **A** to **Z** and **a** to **z** plus the special characters in the ASCII character set.

– With a 64-bit encryption depth, the key is exactly 5 characters long.
  An example of a valid key: GIGA1

– With a 128-bit encryption depth, the key is exactly 13 characters long.
  An example of a valid key: GIGASET_SE551

➔ Enter up to four keys in fields ***Key 1*** to ***Key 4*** and confirm these keys by entering them again in fields ***Confirm key 1*** to ***Confirm key 4***.

➔ Select one of the four keys as ***Default key***.

Please remember:

- It is very **important** that you make a note of the entered or generated key(s). You will need this information to configure the wireless network adapters properly.
- When you have concluded the configuration, you must change the WEP encryption on the wireless network adapters for the connected PCs in the same way as they will not otherwise be given access to the Gigaset SX541 WLAN dsl's wireless network.

➔ Click ***OK*** to apply the settings.

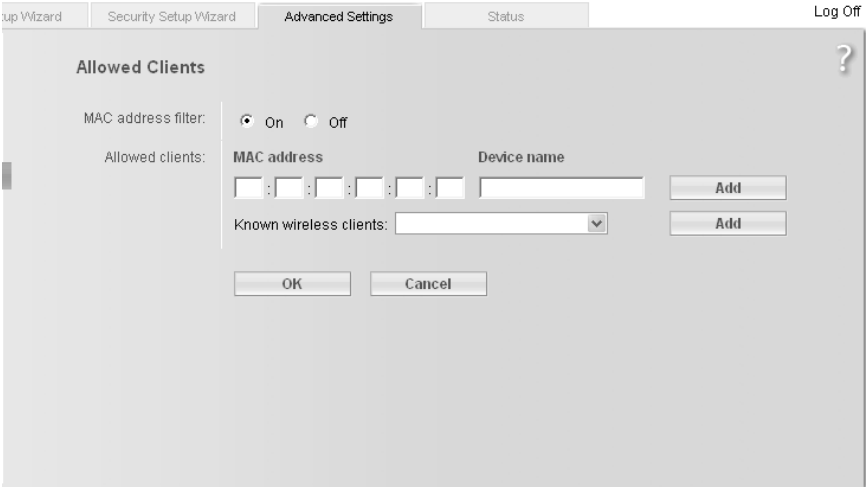
Allowed Clients

You can specify the PCs that are to have wireless access to the Gigaset SX541 WLAN dsl and hence to your LAN on this screen.

In the ***Wireless Network*** menu, select ***Allowed Clients***.The default setting for access control is disabled. This means that all PCs that use the correct SSID can log in.

The access control is based on the MAC addresses of the PCs' network adapters.

➔ Activate access control via the ***On*** option in the ***MAC address filter*** field.



Entering PCs manually:

➔ Enter the required PCs with ***MAC address*** and ***Device name*** in the appropriate fields.

➔ Click the ***Add*** button to add the entry to the list.

➔ Click the ***Delete*** button to delete the entry from the list.

➔ Apply the settings by clicking ***OK***.

Selecting from the list of logged-in PCs

➔ From the ***Known wireless clients*** list (all PCs that currently have access to the Gigaset SX541 WLAN dsl), select the PC you want to add to the access control.

➔ Click the ***Add*** button to add the entry to the list.

➔ Apply the settings by clicking ***OK***.

Please remember:

If you activate MAC access control, you must at least enter the PC from which you are configuring the Gigaset SX541 WLAN dsl. Otherwise you will no longer be able to access the user interface and a corresponding error message will be shown.

If, by mistake, you have denied all PCs access to the Gigaset SX541 WLAN dsl, you have two choices:

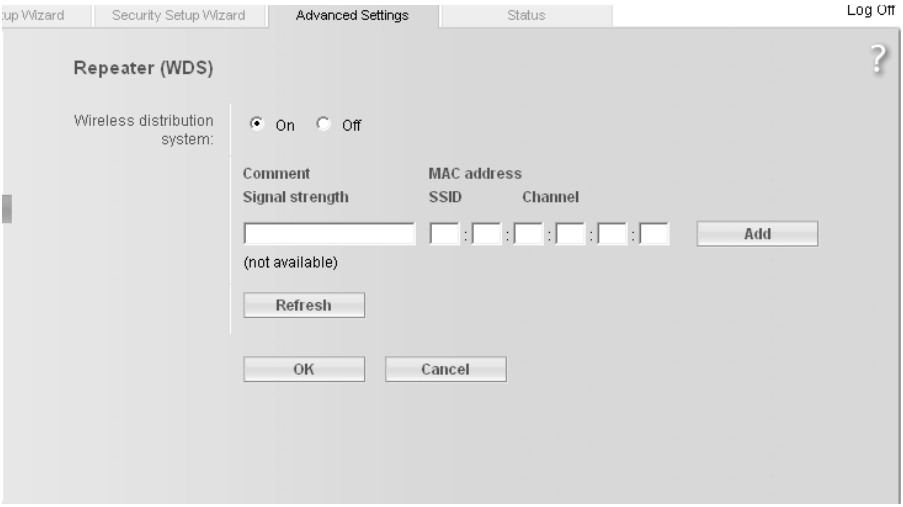
- You can completely reset the Gigaset SX541 WLAN dsl (see page 18).
- You can connect a PC to the Gigaset SX541 WLAN dsl using one of the LAN connections. As MAC access control only applies to PCs that are connected wirelessly, you can use this PC to change the configuration.

Repeater Function (WDS)

If you use a repeater in your wireless network to extend the range, you must activate the Wireless Distribution System (WDS) function.

In the ***Wireless Network*** menu, select ***Repeater (WDS)***.

➔ Next to ***Wireless distribution system***, select the ***On*** option to activate WDS.



The name of the client is shown in the ***Comment*** field.

The MAC address of the repeater is shown in the ***MAC address*** field if there is a connection.

The SSID is shown in the ***SSID*** field if there is a connection with the repeater.

The radio channel used for data transfer is shown in the ***Channel*** field.

The ***Signal strength*** shows the strength of the connection to the repeater in percentage terms if there is a connection to the repeater.

➔ Click ***Refresh*** to update the display.

➔ Click ***Add*** to add the data of another repeater.

➔ Apply the settings by clicking ***OK***.

Setting up Internet telephony (VoIP)

Your Gigaset SX541 WLAN dsl enables you to make telephone calls via the Internet using an analogue phone connected to the Gigaset SX541 WLAN dsl. To do this, you require access authorisation from your service provider and the relevant access data. You must enter this data and other configuration settings for making calls in the ***VoIP*** (Voice over IP) menu in the Advanced Setup.

The menu comprises the following entries:

- VoIP settings: Enter the basic data from your service provider here (see page 105).
- Extensions: Set functions here for two extensions(see page 107).
- Dialing rules: Specify numbers here that are to be called only via the fixed network or only via the Internet. You can block numbers completely (for example 0190 numbers) or enter a call-by-call provider for the fixed network (see page 108).

Please remember:

If you do not specify any of your own dialing rules, then the default settings will be used as entered on the ***Dialing Plans*** screen in the ***VoIP*** menu. All other calls are made via the Internet. If you press the * key twice before dialing the number on the phone, then the call will always be made via the fixed network. The dialing rules will not apply in this case.

Switching over takes a little time. For automatic dialing, insert a pause after the ** by pressing the recall key. You should therefore press: * key, * key, recall key and then the keys for the required phone number.

- Quick dial: Specify quick dial numbers or terms here for phone numbers you use frequently (see page 110).

Important information:

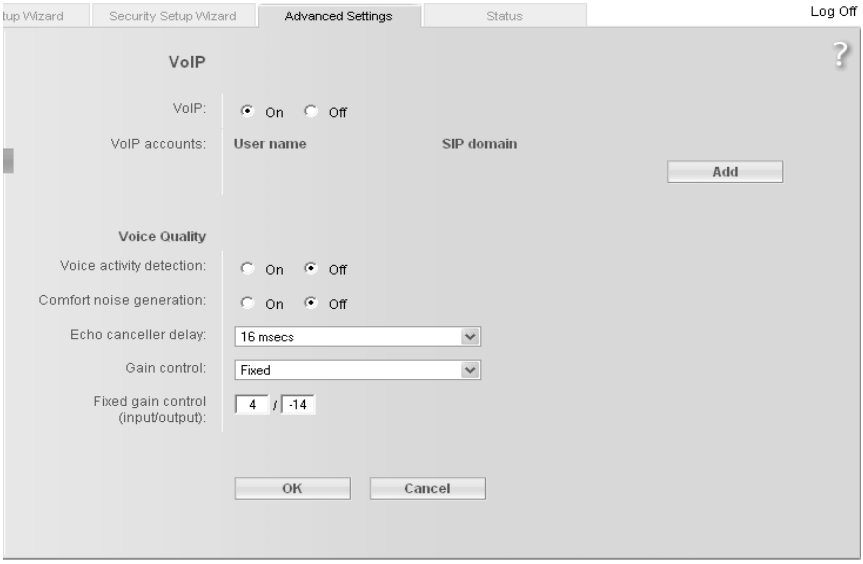
- If VoIP is not set, you will always make calls via the fixed network and the dialing rules (see page 108) will not apply.
- All calls from the fixed network are forwarded to the phone connected to the Phone 1 socket.
- If VoIP is set, then – depending on your provider – a call-by-call number is preset for fixed network calls.
- Please check these dialing rules (see page 108) and amend them if you have agreed special phone tariffs with another provider.

- You should not change the default setting for the connection mode (= "permanent connection") if you are using VoIP (see page 55). You can only be called via VoIP if this setting is used. Please remember, though, that this setting can result in high connection costs if you have agreed a time-based tariff with your Internet provider.
- If there is a power failure, or if you have switched off the Gigaset SX541 WLAN dsl, you can only make calls using a phone connected to the Phone 1 socket. The dialing rules will not apply in this case.

VoiP Settings

You will receive the access and configuration data for Internet telephony from your service provider.

➔ Select ***VoIP*** in the ***Telephony*** menu.



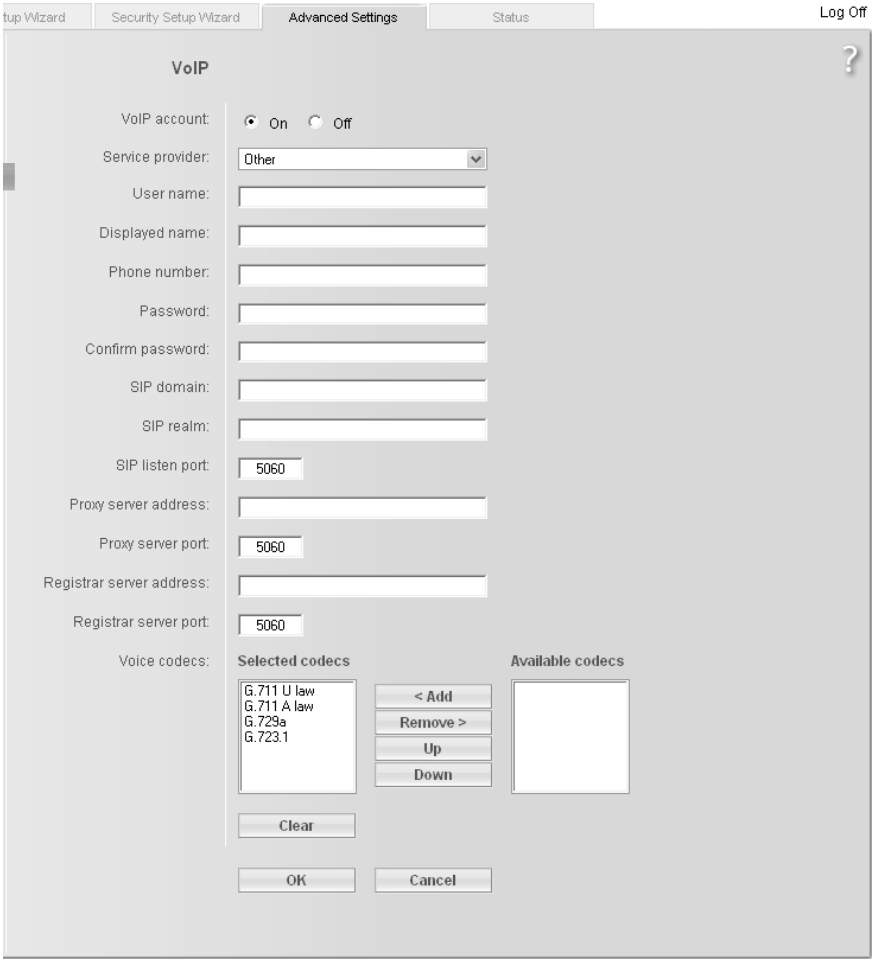
➔ Select ***On*** if you want so use Internet telephony (default setting).

➔ Use the default settings for ***Voice Quality***: ***Voice activity detection***, ***Comfort noise generation***, ***Gain control*** and ***Fixed gain control (input/output)***.

➔ To add the data for your ***VoIP accounts***, click ***Add***.

When you have configured VoIP settings in the Basic Setup Wizard, the data of your VoIP account are shown in this line. You can edit this data or add new data for further accounts.

➔ Click ***On*** to activate the ***VoIP account*** option.



➔ Select ***Other*** from the ***Service provider*** from the selection menu.

➔ Enter the data you have been given by your service provider:

User name, ***Displayed name***, ***Phone number***, ***Password***, ***SIP domain***, ***SIP realm***, ***Proxy server address and Registrar server address***.

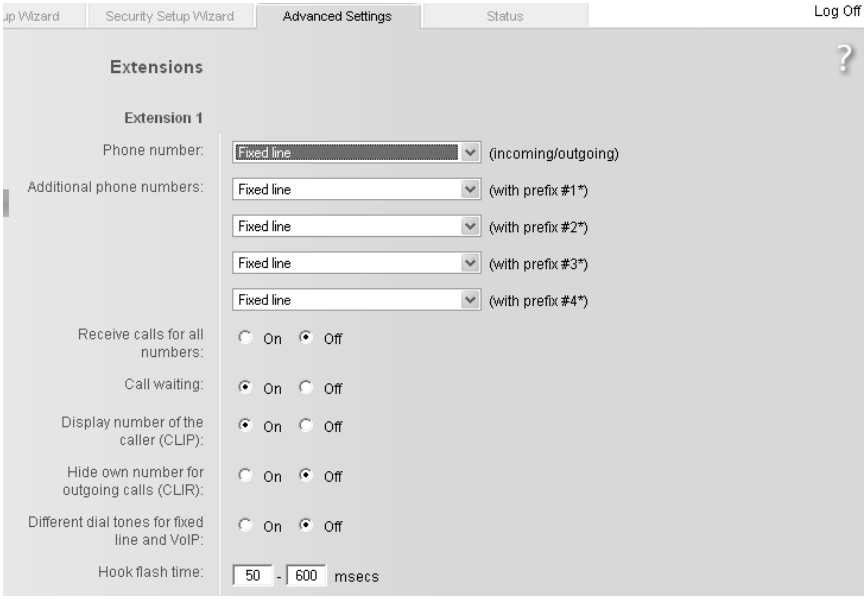
➔ Leave the default settings for the parameters ***SIP listen port***, ***Proxy server port***, ***Registrar server port*** and ***Voice codecs*** unless you have been given other data by your service provider.

➔ Click ***OK*** button to apply the settings.

Extensions

You can assign phone numbers to your extensions and make additional settings for Internet telephony, such as call waiting, display the caller's number and carry out other technical settings.

➡ Select ***Extensions*** in the ***Telephony*** menu.



➡ Select the ***Phone number*** (your service provider or fixed line) from the list for incoming and outgoing calls at extension 1. The list of numbers is the one you have set in the ***VoIP*** menu (see page 105).

➡ Select ***Additional phone numbers***, which you can use for calls at this extension with a prefix.

➡ Select ***Receive calls for all numbers*** if you want to receive all incoming calls at this extension.

➡ Select the ***Call waiting*** option if you want to permit a signal for an incoming call when the lines are busy.

Please remember:

- Call waiting is indicated when you are calling via a VoIP connection and an analogue call is attempting to interrupt this VoIP call.
- Call waiting is **not** indicated for a VoIP call when you are calling via an analogue connection.

➔ If your service provider supports the function, you can have the caller's number displayed via ***Display number of the caller (CLIP)***.

➔ Select ***Hide own number for outgoing calls (CLIR)*** if you want to hide the number of this extension for outgoing calls.

➔ ***Different dial tones for fixed line and VoIP***: If you activate this function, a different dialing tone is used for Internet telephony than for fixed network telephony. This means you can hear immediately when dialing a number whether you are calling via the Internet or via the fixed network.

➔ Leave the default setting for ***Hook flash time*** or change the data.

➔ Select the appropriate settings for extension 2.

➔ Click ***OK*** to apply the settings.

Dialing Plans

On this screen you can

- specify for certain phone numbers or prefixes whether they are to be dialled via the Internet or the fixed network,
- enter a call-by-call provider for the fixed network,
- block phone numbers or prefixes.

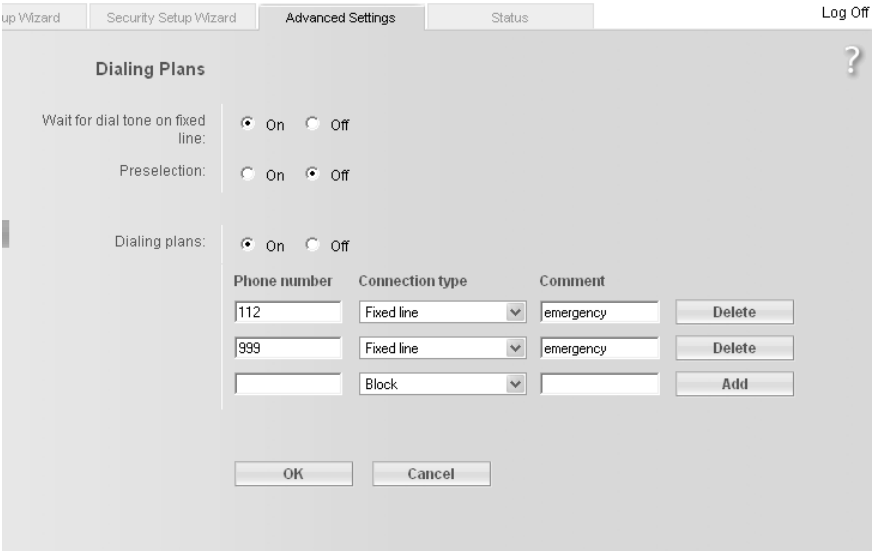
➔ To make these settings, select the menu entry ***Dialing Plans*** in the ***Telephony*** menu.

Please remember:

- If you do not specify dialing rules, the default settings apply. All other calls are made via the Internet. If, however, you press the * key twice before dialing the number on the phone, then the call will always be made via the fixed network.

  Switching over takes a little time. For automatic dialing, insert a pause after the **. Please refer to the user's guide of your telephone, how to insert a pause. You should therefore press: * key, * key, key for pause and then the keys for the required phone number.
- If no VoIP (Internet telephony) is set, you will always make calls via the fixed network and the dialing rules will not apply.
- If VoIP is set, then – depending on your provider – a call-by-call number is preset for fixed network calls.

  Please check these dialing rules and amend them if you have agreed special phone tariffs with another provider.
- If there is a power failure or if you have switched off the Gigaset SX541 WLAN dsl, you can only make calls using a phone connected to the Phone 1 socket. The dialing rules will not apply in this case.



➞ ***Wait for dial tone on fixed line***

When you activate this option, the device is waiting with dialing for a fixed line call until the dial tone is recognized. Otherwise, the first digits of the number may be lost, because it lasts some time to change from Internet telephony to fixed line.

➞ If you want to make all fixed network calls via a call-by-call provider, activate the function ***Preselection***.

➞ Enter the provider's phone number in the field ***Preselection number***.

➞ Phone numbers and prefixes are already entered in the fields for the ***Dialing plans***. You can leave these default settings, overwrite them delete them or add new ones.

➞ In the ***Connection type*** selection field, you can specify whether the entered number is always to be called via the Internet or via the fixed network, or else you can block the number completely.

➞ In the ***Comment*** field, you can enter a description for the number.

➞ Clicking on ***Delete*** removes the whole line and you can add a new line by clicking on the ***Add*** button.

You can define up to a maximum of 32 dialing rules.

➞ Click ***OK*** to confirm the settings.

Quick dial

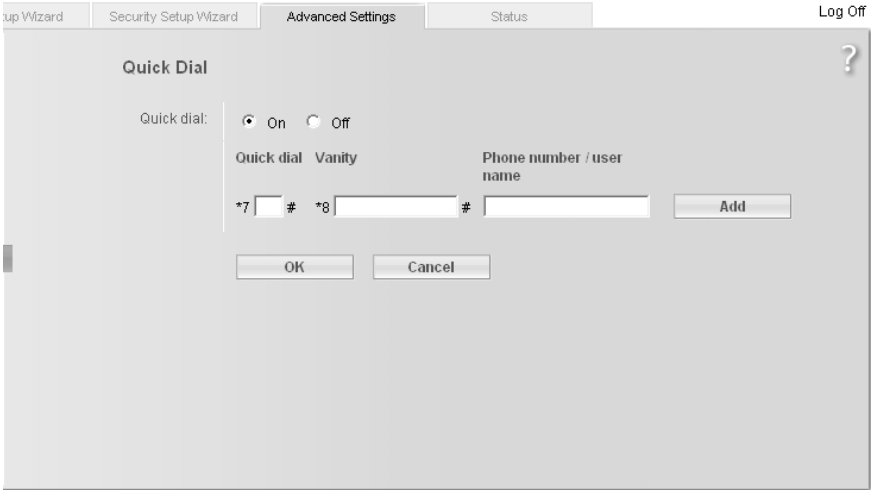
Quick dial numbers or terms enable you to dial frequently used phone numbers quickly and easily.

The quick dial number is a two-digit number (01 to 20). A vanity number is a combination of letters you can enter instead of a phone number. You can specify a quick dial number and/or a vanity number for a phone number.

Start quick dial with the keys *7 quick dial number # and the vanity number with the key combination *8 Vanity #.

➔ To make this setting, select the menu entry ***Quick Dial*** in the ***VoIP*** menu.

➔ Click ***On*** to activate the ***Quick Dial*** option.



➔ Enter the quick dial number in the ***Quick Dial*** field and/or a name or combination of letters in the ***Vanity*** field.

➔ Enter the phone number in the ***Phone number / user name*** field.

➔ Click ***Add*** to save the entry.

More empty lines will then be added.

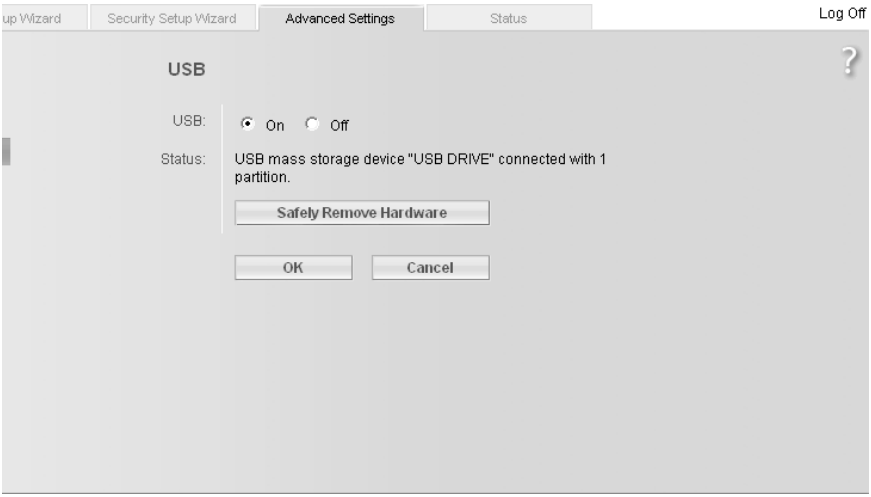
➔ Click ***OK*** to confirm the settings.

USB

You can use your device's USB port to share a USB bulk memory or a USB printer with users in your local network and publish your data on the Internet.

Note:
The Gigaset SX541 WLAN dsl supports USB V1.1. Devices that support USB V2.0 may be connected too.

➔ In the ***Advanced Settings*** menu, select ***USB***.



➔ Activate the USB port on your device.

If a USB device is connected, its ***Status*** is displayed.

Safely Remove Hardware

➔ Click this button and wait until any connected USB bulk memory or USB printer is fully deactivated before disconnecting them from your device.

➔ Click ***OK*** to save the changes.

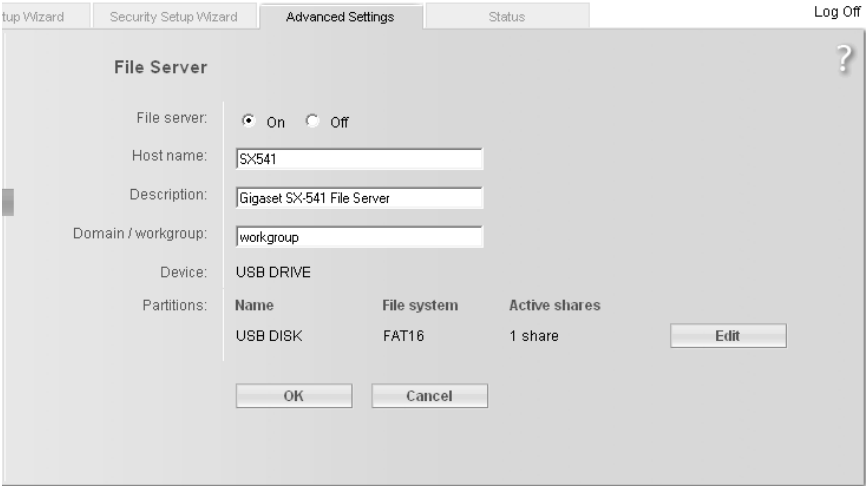
File Server

Your device's integrated file server allows you to make folders and files on a connected USB bulk memory (for example USB stick or USB hard disk) available to all users in your local network.

➔ Connect a USB data carrier to the Gigaset SX541 WLAN dsl via the USB port.

> **Note:**
> The USB interface of the Gigaset SX541 WLAN dsl supplies 480 mA of power. Some hard disks need more power. In this case, the device must have its own mains adapter.

➔ In the ***USB*** menu, select ***File Server***.



➔ Select the ***On*** option for the ***File Server***.

Enter a name for the file server in the ***Host name*** field. This is shown in the network environment of each computer in your local network and allows users to find your file server.

If you assign a name other than ***Server*** (for example the IP address of the Gigaset SX541 WLAN dsl), then the file server will appear in the Windows directory ***Network environment*** both under the name Server and under the name you have assigned.

➔ You can enter a ***Description*** of the file server in the next field.

➔ Enter the name of the ***Domain / workgroup*** (***workgroup*** is the standard name for Windows) in which the file server is located. If you now search your network you will find the file server within the stated domain / workgroup in the network environment.

The connected USB bulk memory is shown in the ***Device*** field.

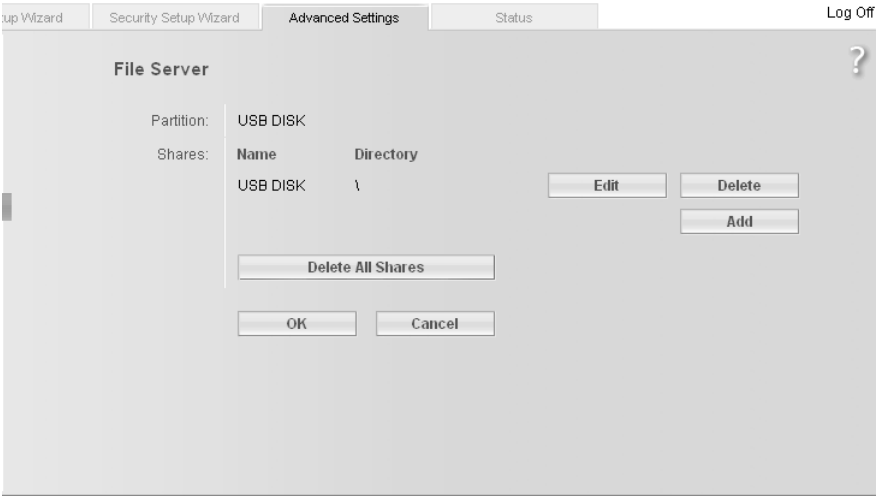
Partitions list and sharing directories

Partitions shows all partitions for the connected data carrier.

➔ Click the ***Edit*** button next to the partition whose directory you want to release for sharing.

> **Note:**
> At most 2 partitions can be released for sharing.

A new window appears with a list of the existing shares.



➔ Click ***Add*** to set up a new share for the partition.

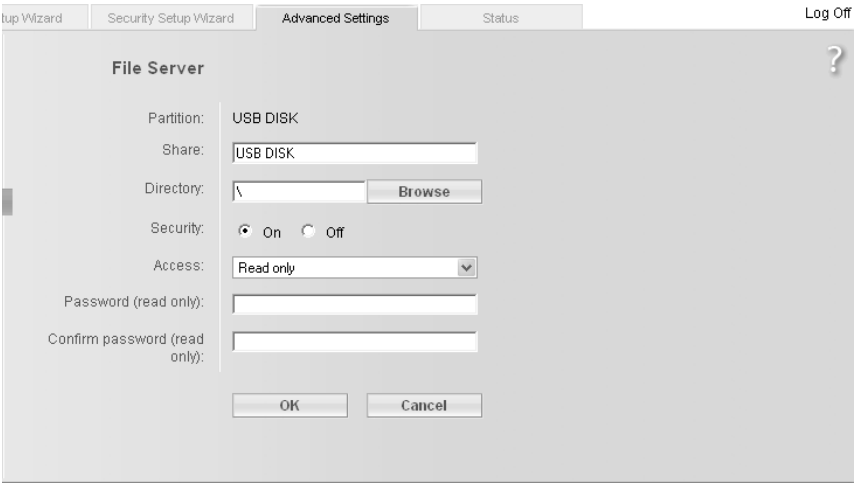
➔ For an existing share, click ***Edit*** to edit the share.

A window opens in both cases for the next steps (see below).

➔ You can delete the required share by clicking on the ***Delete*** button.

➔ Click ***Delete All Shares*** if you wish to cancel all existing shares.

Setting up or editing a share



➔ Enter a name for the ***Share***.

➔ Select the directory you wish to release for sharing. You can enter the complete path for the directory manually or click the ***Browse*** button. A file menu is opened.

You can now set access protection for the directory.

➔ First, select the ***On*** option for ***Security***.

➔ Select the required option from the list next to ***Access***:

- Select ***Read only*** if you only wish to release the data for reading.
- Select ***Full control*** if you wish to release the data for reading and writing.

➔ Select ***Depending on password*** if you wish to make access dependent on a password.

Depending on the access option chosen, you can now a password for read only or a password for full control enter in the relevant field or else different passwords for both read only and full control.

➔ Now enter the password or words and confirm by entering it/them again.

➔ Click ***OK*** to save your settings.

Web Server

Your device's integrated Web server allows you to publish data on a connected USB bulk memory (for example USB stick or USB hard disk) on the Internet.

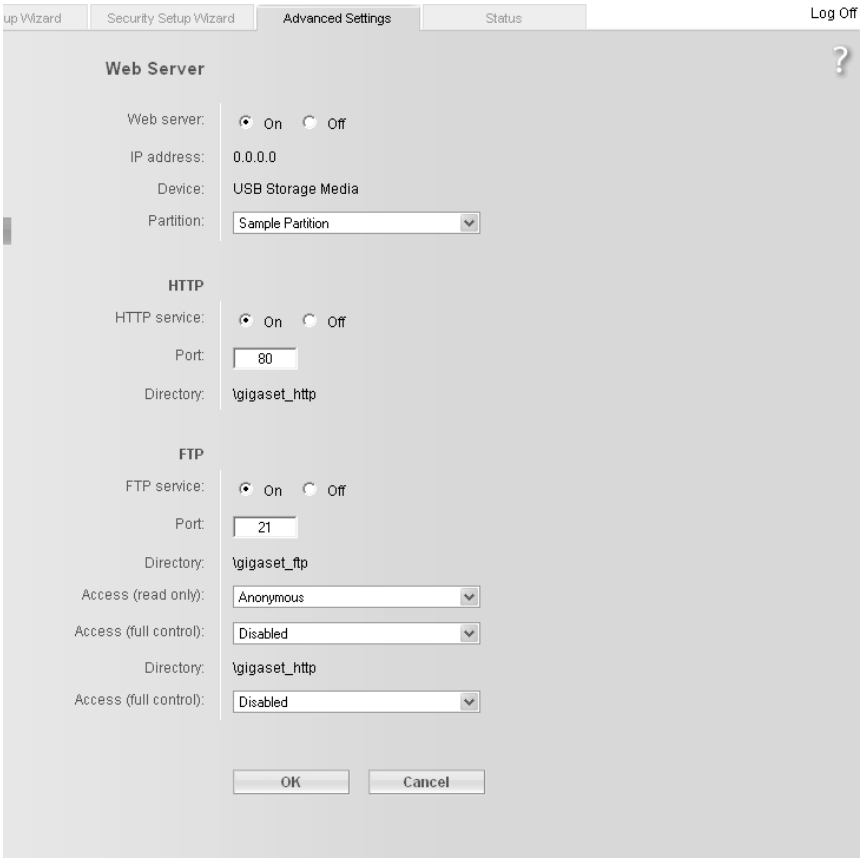
Internet users can access your Web server by entering the public IP address in their Internet browser. As Internet providers often change this each time someone dials in, it is worth using dynamic DNS (see page 90) in addition.

➔ Connect a USB data carrier to the Gigaset SX541 WLAN dsl via the USB port.

You can check the status of the connection to the USB bulk memory on the ***Advanced Settings*** – ***USB*** screen.

➔ In the ***Advanced Settings*** menu, select ***Web Server***.

➔ Activate your device's integrated Web server.



➔ Select the ***Partition*** on the connected data carrier to which you wish to save the data for the Web server.

HTTP

HTTP (Hypertext Transfer Protocol) is the standard protocol for transferring data on the Internet. You can use it, for example, to publish your own homepage on the Internet.

➔ Activate the HTTP service for your Web server.

➔ You can change the ***Port*** via which Internet users can access your data, for example, to hide your data and protect it from unauthorised users.

For your security, it is only possible to publish data on the Internet via the HTTP service if this is stored in the ***\gigaset_http*** directory.

FTP

FTP (File Transfer Protocol) is a protocol for exchanging files on the Internet. You can use it, for example, to offer files for downloading or to receive files from other users.

➔ Activate the FTP service for your Web server.

➔ You can change the ***Port*** via which Internet users can access your data, for example, to hide your data and protect it from unauthorised users.

For your security, it is only possible to publish data on the Internet via the FTP service if this is stored in the ***\gigaset_ftp*** directory.

In addition – for example, if you wish to change your own homepage via the Internet – you can also set up FTP access in the ***\gigaset_http*** directory. You can allow this access generally or only allow it for selected users with a user name and password.

➔ For ***Access (read only)***, select whether all users may read your data in ***Anonymous*** mode or only one ***Specified user***.

➔ Select whether ***Access (full control)*** to your data is ***disabled*** or whether a ***Specified user*** may read, edit and delete your data.

➔ Enter the name in the ***Specified user*** field. Define different user names for the different types of access and directory.

➔ Enter the password for the user and confirm it by entering it again in the field below. Please note when making the entry that the password is case sensitive. Avoid proper names and all too obvious words. Instead, use upper and lower case letters, numbers and special characters.

➔ Click ***OK*** to apply the changes.

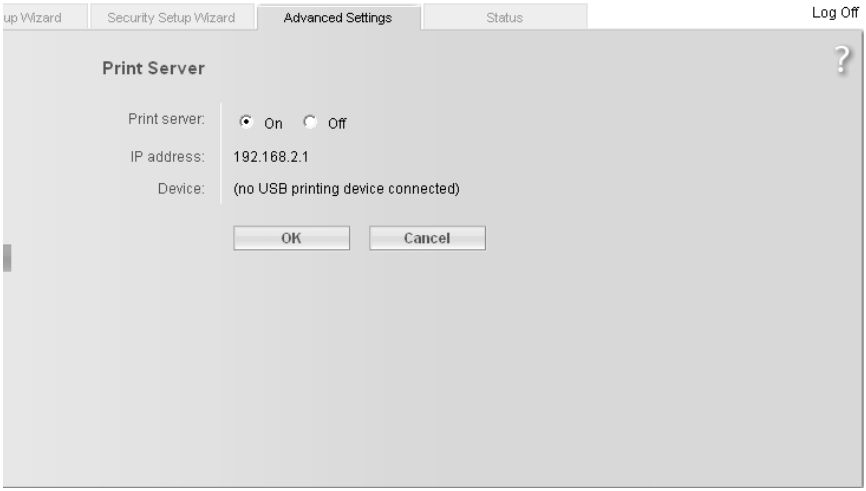
Print Server

Your device's integrated printer server allows you to offer a USB printer to all users in your local network.

Note:
At present, the printer server can only be used with selected printers. You can obtain further information by contacting the hotline or else on the Internet (see Quick Start Guide).

To be able to use this function, first connect a USB printer to the USB port on your device such that this device is shown on this screen. You can check the status of the connection to the USB printer on the ***Advanced Settings*** – ***USB*** screen.

➔ Activate your device's integrated printer server.



Users can set up the connected printer by entering the local ***IP address*** on your PC.

➔ Click ***OK*** to accept the changes.

You will find information on setting up the printer connected to the Gigaset SX541 WLAN dsl in the section entitled "Installing the Printer Port for Network Printers" on page 139.

Administration and Status Information

The Gigaset SX541 WLAN dsl user interface includes several helpful functions for administration. You can

- open an Internet connection manually (see below),
- make regional settings (see page 119),
- change the system password (see page 120),
- set up remote management (see page 121),
- save and, if necessary, restore configuration data (see page 123),
- reset the Gigaset SX541 WLAN dsl to the factory settings (see page 124),
- reboot the device (see page 124),
- update the firmware (see page 125),
- make the settings for the system protocol (see page 126),
- view information about the configuration and status of the Gigaset SX541 WLAN dsl (see page 127).

Connecting to the Internet Manually

You can connect to the Internet manually. If, for example, you deactivated the function Auto Connect when configuring Internet access, then Internet applications (such as your browser or e-mail application) will not automatically open a connection when they are launched. In this case, you will have to open the connection manually when it is required and also close it again when you are finished with it.

To open or close an Internet connection manually:

➔ Open the Gigaset SX541 WLAN dsl start screen as described on page 48.

If you have already started the configuration environment, click the start screen tab at the top left of the window.

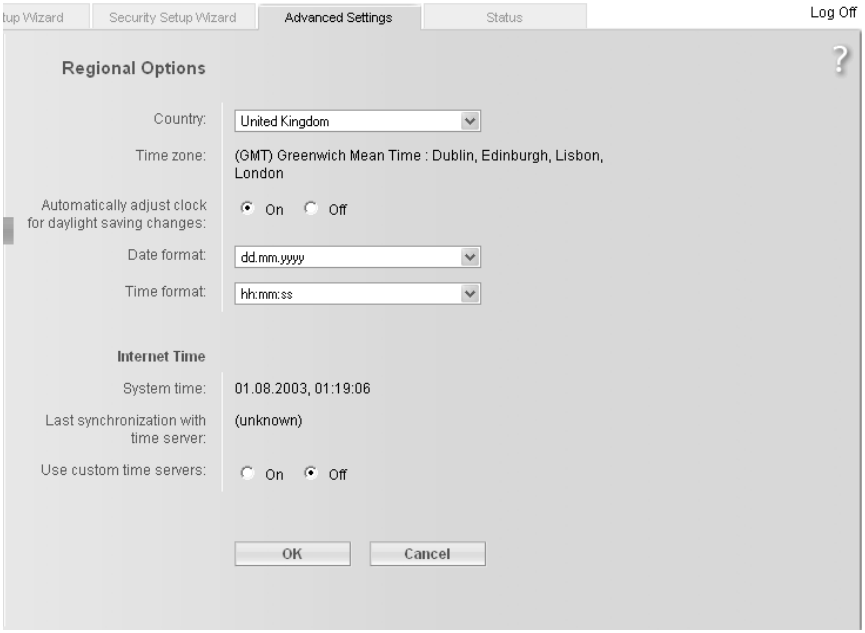
If you have not yet started the configuration environment, start it now and log on.

➔ Click ***Connect*** to open a connection to the Internet.

Regional Options

To operate your Gigaset SX541 WLAN dsl, you can select the location, time zone and the format for entering the date and time, as well as configure the application for a time server for the Internet time.

➔ In the ***Advanced Settings*** – ***Administration*** menu, select the entry ***Regional Options***.



➔ Select the country where you are currently located from the list. You can make the settings for the clock to change automatically to summer time and/or to the ***Time zone*** as you wish.

➔ Select the required option and/or select the ***Time zone*** for your location.

➔ Select the required format for entering the date and time from the ***Date format*** and ***Time format*** lists respectively.

Internet Time

The ***System time*** for your device is automatically synchronised with the time server on the Internet. The time of the ***Last synchronization with time server*** is displayed for your information.

➔ If you wish to use your own time server, select the ***On*** option next to the ***Use custom time servers*** field.

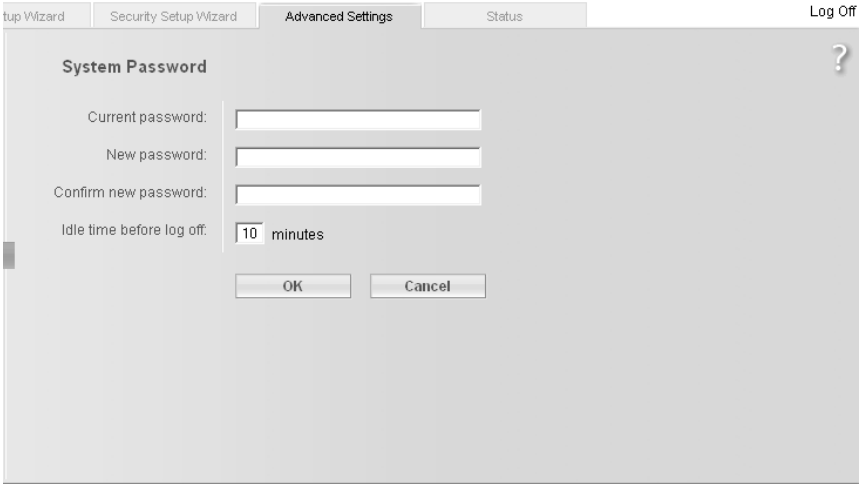
➔ Enter the Internet address for the time server in the ***Preferred time server*** and ***Alternate time server*** fields respectively.

➔ Click ***OK*** to apply the settings.

System Password

You can assign a System Password for the configuration environment of your Gigaset SX541 WLAN dsl and specify the period after which a session is to end automatically if no further entry is made.

➔ In the ***Administration*** menu, select ***System Password***.



After installation, the configuration of the Gigaset SX541 WLAN dsl is protected with the System Password **admin**. To prevent unauthorised changes to the configuration, you should change this System Password from time to time. You may have already set a System Password when setting up the ***Security Setup Wizard***. If so, you can change it here.

➔ Enter the old System Password in the ***Current password*** field.

➔ Enter a new password in the ***New password*** field and repeat it in the ***Confirm new password*** field.

The password may contain up to 12 characters. The password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters, numbers and special characters.

Please remember:

If you ever forget your System Password, you will have to reset your Gigaset SX541 WLAN dsl (see page 18). Please bear in mind that this will restore **all** the settings to the factory configuration. No System Password will be active either.

Setting Idle time before log off:

➔ Enter the period in minutes after which the configuration program is to be aborted if no entry is made. The default setting is 10 minutes. If you enter the value 0, the program will never be aborted automatically.

➔ Click ***OK*** to accept the settings.

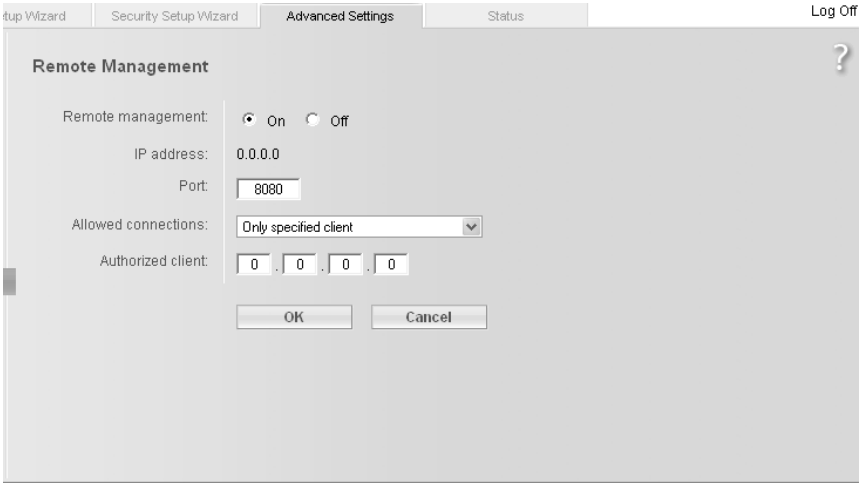
Setting up Remote Management

Remote Management enables a PC that is not in your local network to be used to configure the Gigaset SX541 WLAN dsl with a standard Web browser. You can permit Remote Management for one particular PC or for any PCs.

For security reasons, this function is only available if you have previously changed the system password for your device (see page 120).

➔ In the ***Administration*** menu, select ***Remote Management***.

➔ Select the ***On*** option for ***Remote Management*** if you wish to permit Remote Management.



You can start remote management by entering the public IP address in your Internet browser. As Internet providers often change this each time you dial in, it is worth using dynamic DNS (see page 90) in addition.

➔ You can change the ***Port*** via which you can access the configuration program from the Internet, for example in order to hide and protect the configuration program against unauthorised access.

➔ ***Allowed connections:*** You can specify one particular PC for Remote Management or permit this function for any PCs. Select the required option from the list.

Please remember:

If you permit several PCs then anyone who finds out your password can access this user interface and therefore also your network! If it is needed, then you should only activate this option for a short time.

Remote Management for one particular PC:

➔ In the ***Authorized client*** field, enter the IP address of the PC that is to have access to the user interface of the Gigaset SX541 WLAN dsl from outside your local network.

Please remember:

- The Internet provider might assign the IP address to the PC dynamically. This can then change the IP address. Make sure that the PC that is to access the router from the Internet always has the same IP address.
- For access to the configuration environment via Remote Management, you must enter the address of the Gigaset SX541 WLAN dsl to be managed in the browser using the following format: **`http://x.x.x.x:8080`** (x.x.x.x stands for the IP address of the Gigaset SX541 WLAN dsl).

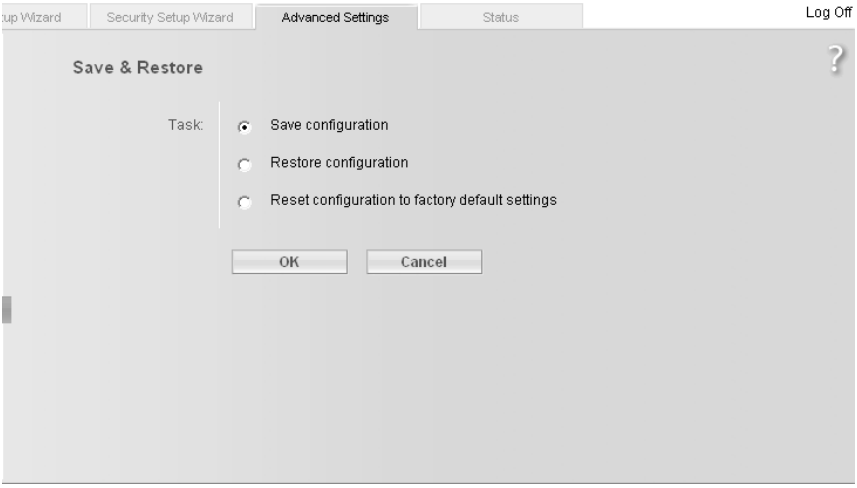
➔ Click ***OK*** to accept the settings.

Saving and Restoring a Configuration

Once you have configured your Gigaset SX541 WLAN dsl, it is advisable to back up the settings. You can then restore them at any time, should they be accidentally deleted or overwritten.

You can also reset the configuration to the factory settings. You should always do this before passing your device on to any outsiders.

◆ In the ***Administration*** menu, select ***Save & Restore***.



Saving Configuration Data

➡ For ***Task,*** select the option ***Save configuration***.

This opens a file selection window where you can specify the file you wish to store in the backup file.

➡ Select a directory on your local PC where you wish to store the configuration file and enter a name for the file.

➡ Click ***Save***.

Once the procedure has been completed, the current configuration data will have been backed up in the specified file.

Restoring the Back-up

➔ For ***Task,*** select the option ***Restore configuration.***

➔ Select the backup file in your file system that you wish to use to restore the configuration.

A window will appear prompting you to confirm the procedure.

➔ Click ***OK***. The configuration will now be updated.

Resetting to the Factory Settings

You can reset the Gigaset SX541 WLAN dsl to the factory settings. You should do this before making the device available to others or exchanging it through the dealer. Otherwise unauthorised persons may use your Internet access data at your expense.

➔ Select the option ***Reset configuration to factory default settings*** and click ***OK***.

A window will appear prompting you to confirm the procedure.

Please remember:

You can restart your Gigaset SX541 WLAN dsl if it is not working properly. It should then be ready for use again (see page 18).

Please bear in mind that when the device is fully reset, **all** configuration settings will return to the factory settings. This means that you will have to completely reconfigure the Gigaset SX541 WLAN dsl.

Reboot

You can restart your Gigaset SX541 WLAN dsl if it is not working properly. It should then be ready for use again.

In the ***Administration*** menu, select ***Reboot***.

Click ***OK*** to restart the device.

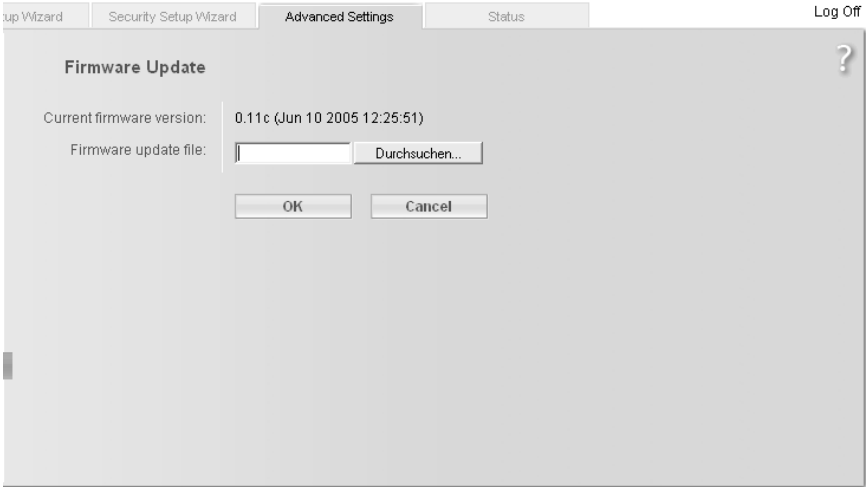
Updating Firmware

If Siemens or your Internet provider make a new version of the firmware available, you can update the firmware of the Gigaset SX541 WLAN dsl. To do this, you must first download the new firmware into your PC.

Then proceed as follows:

➔ Close down all network activities in your local network.

➔ In the ***Administration*** menu, select ***Firmware Update***.



The version of the firmware currently running on your device is displayed in the line ***Current firmware version***.

➔ In the ***Firmware update file*** field, enter the file with the new firmware you have downloaded from the Internet.

➔ Click ***OK***.

The firmware will now be updated.

Please remember:

Do not switch off your Gigaset SX541 WLAN dsl during the updating procedure. Updating can take several minutes.

After successful updating, the device is automatically rebooted. All the LEDs will go out. After successful updating, the login screen appears again.

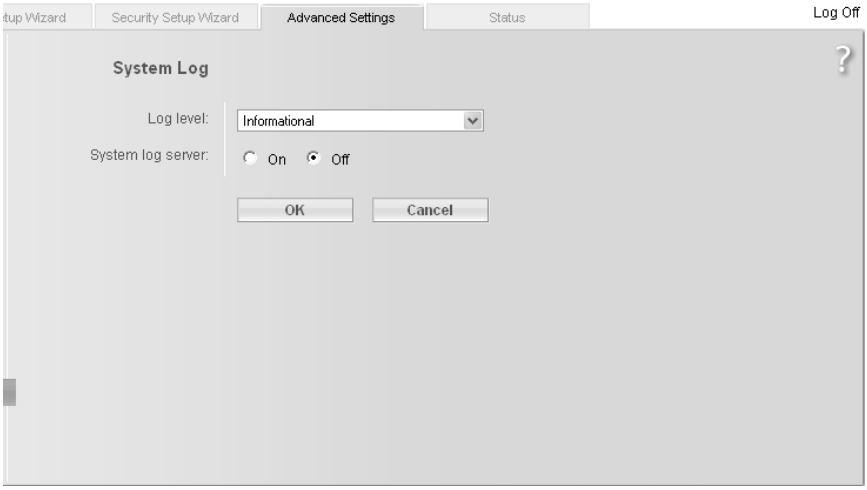
Please remember:

You can check whether the upgrade process was in fact successful in the ***Status*** menu on the start screen (see page 127). You should see the latest firmware version for the Gigaset SX541 WLAN dsl here.

System Log

The System Log is displayed in the ***Status*** – ***Device*** menu. It can give you important information about the functioning of your device and possible problems. You can also have this information transmitted automatically to a system log server.

➔ In the ***Administration*** menu, select ***System Log*** to make the settings for the log.



➔ ***Log level***: Select how much information is to be contained in the system log. You can choose between four levels:

- ***Critical***: logs the most important information concerning possible problems in the functioning of your device
- ***Debugging***:complete and detailed information about all your device's functions
- ***Warning*** and ***Informational*** are intermediate levels.

➔ ***System log server***

- Activate this function if you require automatic transmission of your device's system log to a system log server in your local network.
- ***Server address***:
  Enter the IP address for the system log server.
- ***Server port***:
  Enter the port of the system log server that is to be used to transmit the system log.

➔ Click ***OK*** to save and apply the changes.

Status Information

You can view information about the configuration and status of the Gigaset SX541 WLAN dsl in the ***Status*** menu of the Gigaset SX541 WLAN dsl. You will see an overview of the status of the Internet connection, the local and wireless network and of the device on the first screen.

For detailed information you can view the following status screens:

- ***Security***
- ***Internet***
- ***Traffic Control***
- ***Local Network***
- ***Wireless Network***
- ***Telephony***
- ***Device***

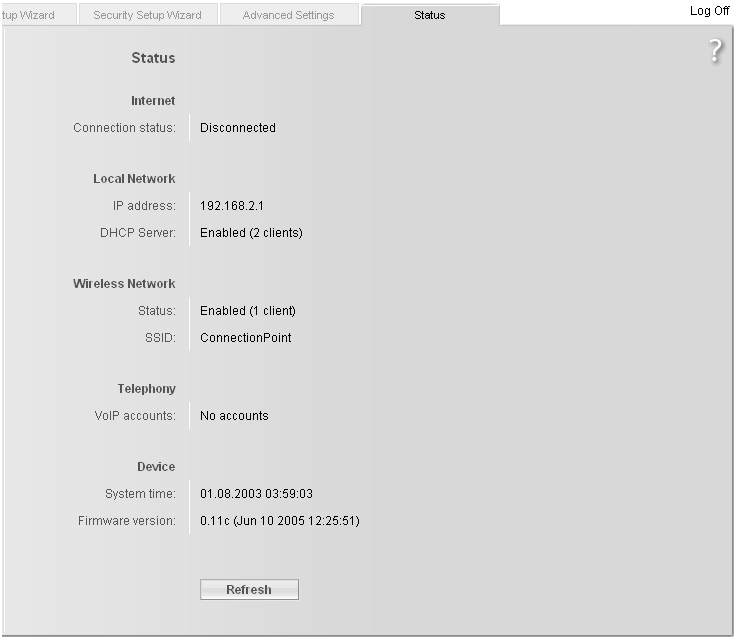
To display a status screen, proceed as follows:

➔ Select ***Status*** on the start screen.

➔ Select the entry with the information you require.

Overview

You are given an overview of the current operating status and most important data for your device on the first screen.



Internet

- ***Connection status***
  The status of the connection to the Internet and, if connected, the duration of the connection.
- ***IP address***
  The public IP address of your device.

Local network

- ***IP address***
  The local IP address of your device.
- ***DHCP Server***
  The status of the DHCP server for your device and, if activated, the number of clients in your network to which an IP address has been assigned.

Wireless network

- ***Status***
  The status of the wireless network connection for your device and, if activated, the number of clients in your wireless network connected to your device.
- ***SSID***
  The identification of your wireless network.
- ***Telephony***
  Your VoiP accounts.

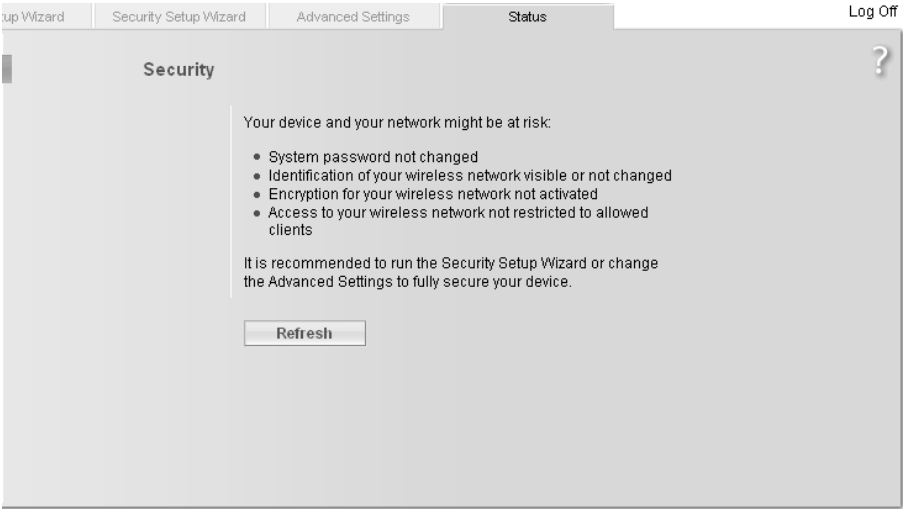
Device

- ***System time***
  Your device's system time.
- ***Firmware version***
  The version of the firmware currently installed in your device.

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Security

On the ***Security*** screen in the ***Status*** menu you will see information about possible security risks for your device and your network.


Security Setup Wizard
Advanced Settings
Status
Log Off
Security
Your device and your network might be at risk:
System password not changed
Identification of your wireless network visible or not changed
Encryption for your wireless network not activated
Access to your wireless network not restricted to allowed clients
It is recommended to run the Security Setup Wizard or change the Advanced Settings to fully secure your device.
Refresh

- ***System password not changed***

  Your device's configuration program is not effectively protected against unauthorised access, as you have either not changed the password since setting the device up or you have not assigned any password at all. The section entitled "System Password" on page 120 describes how to avoid this security risk.

- ***Identification of your wireless network visible or not changed***

  Unauthorised users can also find your wireless network easily as you have not changed the ID for your wireless network (SSID) since setup and have not deactivated the broadcasting of the SSID (SSID broadcast). The section entitled "Configuring Wireless Connections" on page 95 describes how to avoid this security risk.

- ***Encryption for your wireless network not activated***

  None of the data in your wireless network is encrypted when transmitted and can therefore easily be intercepted. Unauthorised users can also easily access your network, your PCs and your Internet connection by this means. The section entitled "Setting Wireless Security" on page 97 describes how to avoid this security risk.

- ***Access to your wireless network not restricted to allowed clients***

  Users can access your wireless network from any PC. The section entitled "Allowed Clients" on page 102 describes how to avoid this security risk.

- ***Firewall for your Internet connection turned off***

  Your network is not protected against hackers making unauthorised access from the Internet. The section entitled "Firewall" on page 78 describes how to avoid this security risk.

- ***Address translation for your Internet connection turned off***

  The clients in your network are not protected against unauthorised access from the Internet. The section entitled "Setting up the NAT Function" on page 85 describes how to avoid this security risk.

- ***One or more of your local clients directly exposed to the Internet***

  One or more clients in your network are directly visible to the Internet as exposed hosts and therefore particularly exposed to risk (for example from hacker attacks). You should only activate this function if it is absolutely necessary (e.g. to operate a Web server) and other functions (e.g. port forwarding) are not adequate. In this case, you should take appropriate measures on the clients concerned. The section entitled "Opening the Firewall for Selected PCs (Exposed Host)" on page 89 describes how to avoid this security risk.

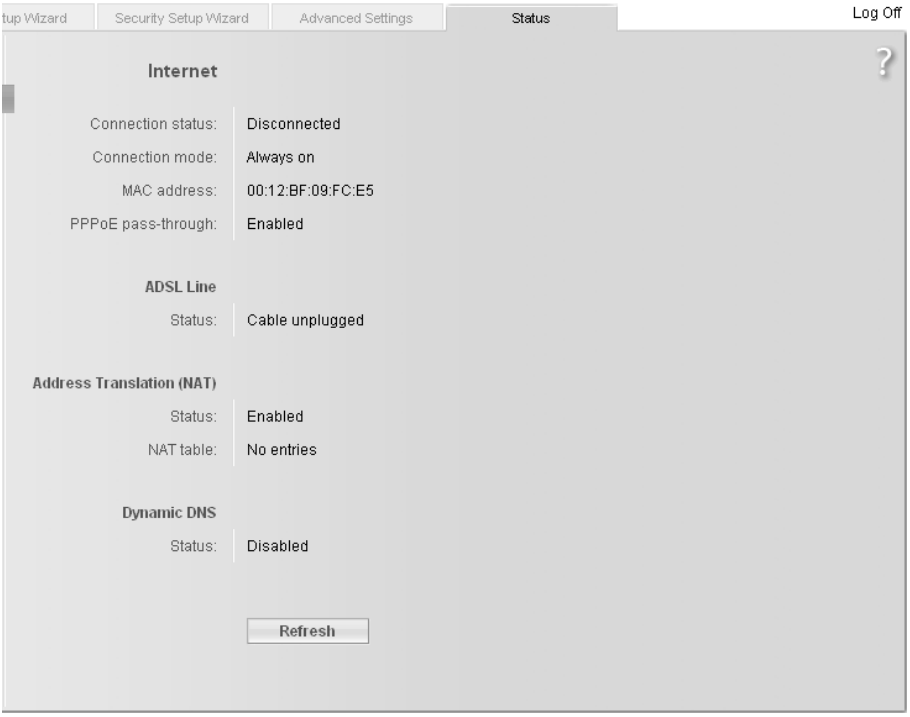
- ***Remote management enabled***

  Any user, including unauthorised ones, who gains knowledge of the system password for your device can access your device's configuration program via the Internet. The section entitled "Setting up Remote Management" on page 121 describes how to avoid this security risk.

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Internet

On the ***Internet*** screen in the ***Status*** menu, you will find information about the status of your device's Internet connection.



- ***Connection status***

  Shows the status of the connection to the Internet and, if connected, the duration of the connection. If you have set ***Connect on demand*** or ***Connect manually*** as the connection mode (see page 70), you can ***Connect*** or ***Disconnect*** the connection to the Internet manually here.

- ***Connection mode***

  The connection mode set for connecting to the Internet.

- ***IP address***

  Shows the public IP address of your device.

- ***MAC address***

  Shows the public MAC address of your device.

- ***Default gateway***

  Shows the IP address of the default gateway used for the current Internet connection.

- ***Preferred DNS server***

  Shows the IP address of the preferred DNS server used for the current Internet connection.

- ***Alternate DNS server***

  Shows the IP address of the alternative DNS server used for the current Internet connection.

- ***Downstream rate***

  Shows the transmission rate of the current Internet connection for downloads from the Internet.

- ***Upstream rate***

  Shows the transmission rate of the current Internet connection for uploads to the Internet.

- ***PPPoE pass-through***

  Shows the status of PPPoE pass-through for your DSL or cable connection for establishing Internet connections straight from a PC to your network.

- ***Address Translation (NAT)***
  - ***Status***

    Shows the status of NAT (Network Address Translation) for your Internet connection.
  - ***NAT table***

    Shows the number of entries currently existing in the NAT table.

    Click ***Empty*** to delete all currently existing entries in the NAT table.
- ***Dynamic DNS***
  - ***Dynamic DNS***

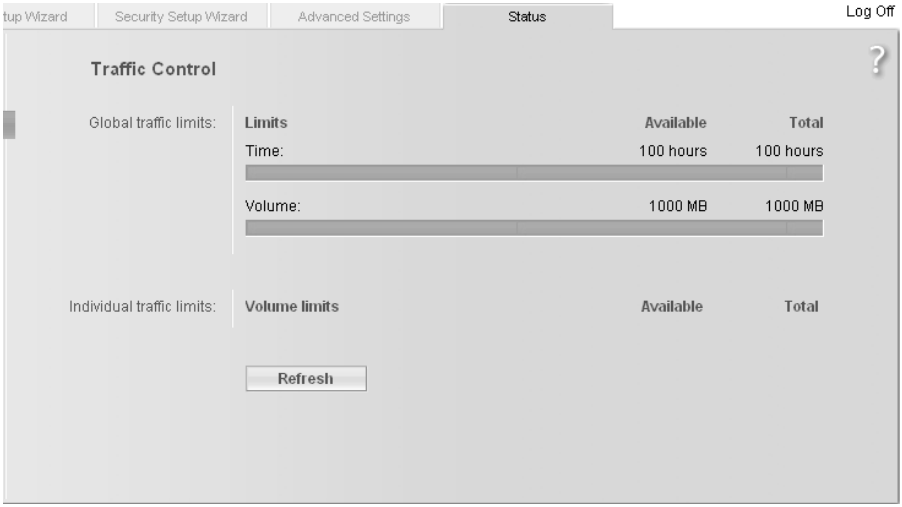
    Shows the status of the dynamic DNS for your Internet connection.
  - ***Domain name***

    Shows the domain name set for dynamic DNS.

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Traffic Control

You will see information about limits and the time and data volume currently available for your Internet connection in the ***Status*** menu on the ***Traffic Control*** screen.



➔ Click ***Refresh*** to refresh this screen and update the displayed data.

- ***Global traffic limits***
  - ***Time***

    The bar indicates the remaining time available to all users in your network for surfing the Internet this month. On the right you will find the relevant details of the total time available per month (***Total***) and the time still available for this month (***Available***) in hours.
  - ***Volume***

    The bar indicates the remaining data volume available to all users in your network for surfing the Internet this month (downloads and uploads). On the right you will find the relevant details of the total data volume available per month (***Total***) and the data volume still available for this month (***Available***) in megabytes (MB).
- ***Individual traffic limits***

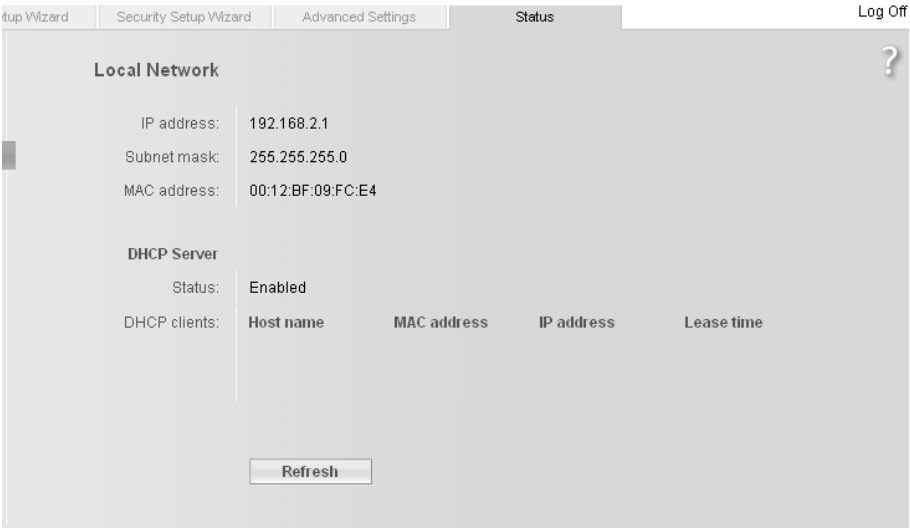
  The bar indicates the remaining data volume available to the PC concerned for surfing the Internet this month (downloads and uploads). The MAC address and computer name are displayed to identify the PC. On the right you will find the relevant details of the total data volume available per month (***Total***) and the data volume still available for this month (***Available***) in megabytes (MB).

Please remember:

The values recorded by your device for online time and transmitted data volume are only intended for your guidance and may differ from the values determined by your Internet provider.

Local Network

You will find information about the settings for your local network in the ***Status*** menu on the ***Local Network*** screen.



- ***IP address***

  Shows the local IP address of your device.

- ***Subnet mask***

  Shows the subnet mask used in the local network.

- ***MAC address***

  Shows the local MAC address of your device for wired data transmission.

- ***DHCP Server***

  – ***Status***

  Shows the status of the DHCP server for your device for automatic assignment of IP addresses to clients in your local network.

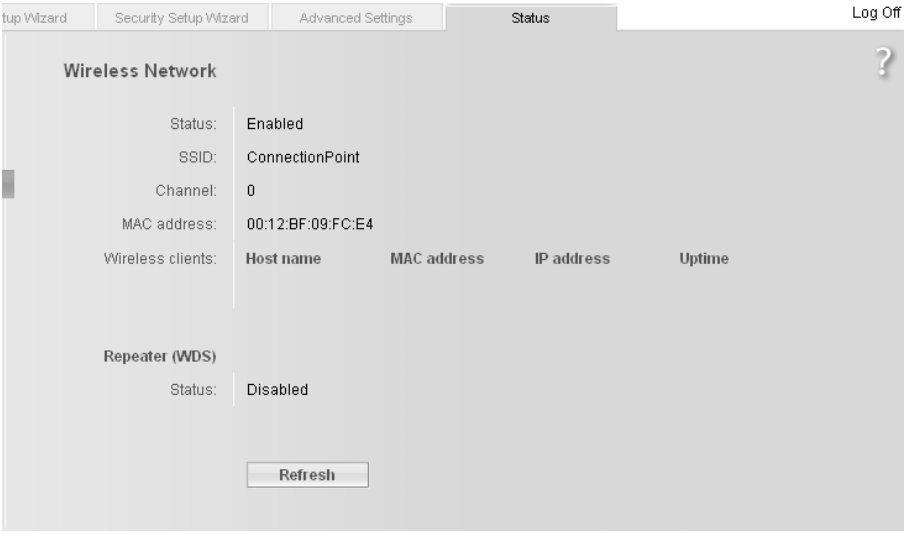
- ***DHCP clients***

  Shows all clients in your network that have been assigned an IP address. The ***Host name*** and the ***MAC address*** of each client are listed for identification. You are also given information about the ***IP address*** assigned to each client as well as the remaining ***Lease time*** for the IP address before the client is assigned a new address by the DHCP server.

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Wireless Network

You will find information about the settings for your wireless network in the ***Status*** menu on the ***Wireless Network*** screen.



- ***Status***
  Shows the status of the connection between your device and the wireless network.
- ***SSID***
  Shows the identification of your wireless network.
- ***Channel***
  Shows the radio channel currently used for transmitting data within your wireless network.
- ***MAC address***
  Shows the local MAC address of your device for wireless data transmission.
- ***Wireless clients***
  Shows all clients in your wireless network currently connected to your device. The ***Host name***, the ***MAC address*** and the ***IP address*** of each client are listed for identification. You will also see information about the ***Uptime*** to date of the current connection for each client in your wireless network.

- ***Repeater (WDS)***
  - ***Status***

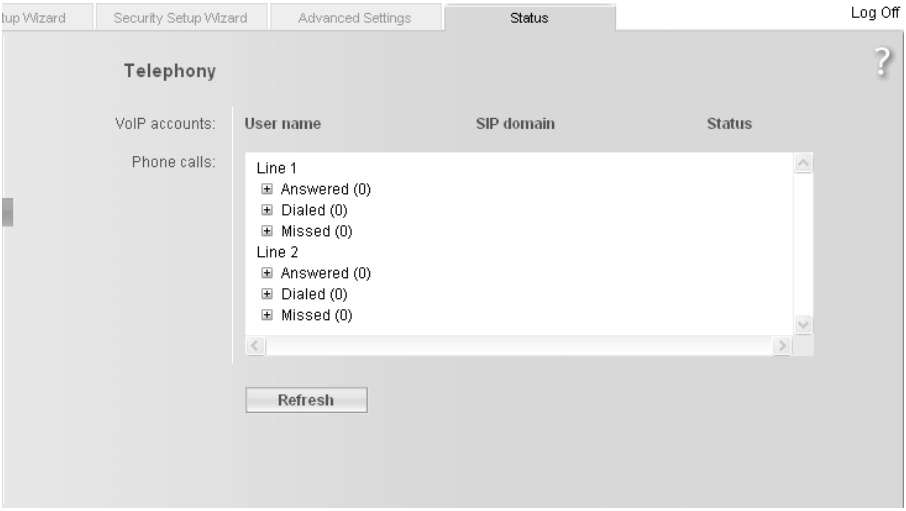
    Shows the status of the WDS (Wireless Distribution System) in your wireless network for increasing the range.
  - ***WDS links***

    Shows the current number of existing connections to other access points or repeaters in your wireless network.

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Telephony

On the ***Telephony*** screen in the ***Status*** menu you will find information about your VoIP accounts and a statistic of your phone calls.



- ***VoIP accounts***

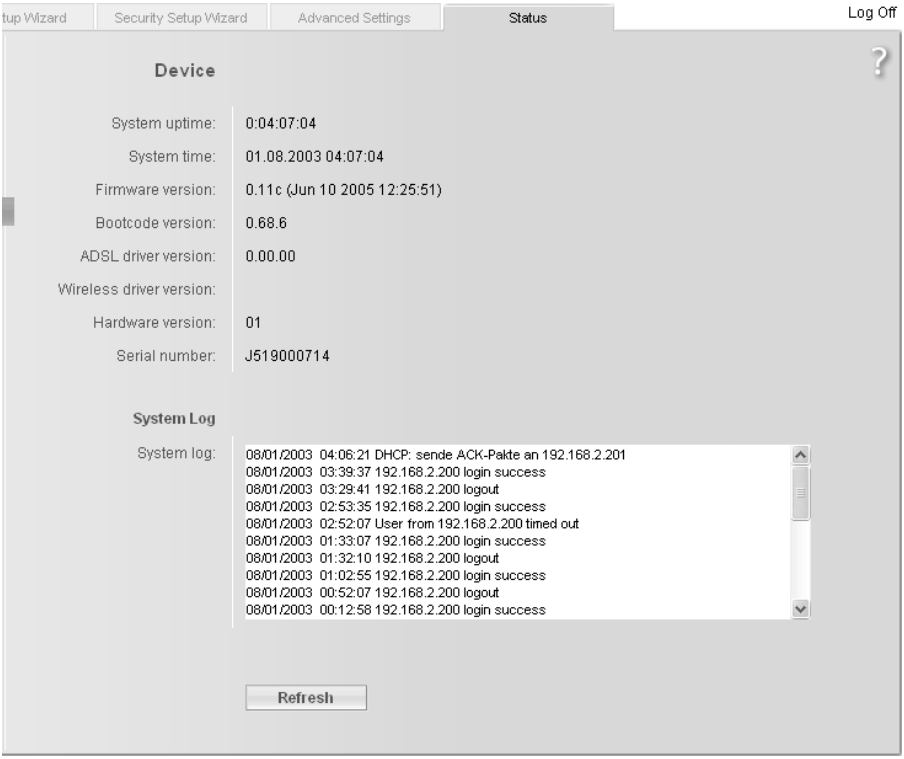
  Shows the data an status of your VoIP accounts.
- ***Phone calls***

  Shows for the two lines all phone calls: answered, dialed and missed calls. If you click one type of calls, the tree is opened and all calls are shown.

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Device

You will find information about the most important data for your device in the ***Status*** menu on the ***Device*** screen.



- ***System uptime***
  Shows your device's operating time since the last time the system was started.
- ***System time***
  Shows the system time for your device.
- ***Firmware version***
  Shows the version of the firmware currently installed in your device.
- ***Bootcode version***
  Shows the version of the boot code currently installed in your device.
- ***Wireless driver version***
  Shows the version of the WLAN driver currently installed in your device.
- ***Hardware version***
  Shows the version of your device's hardware.

- ***Serial number***

  Shows your device's serial number.

- ***System Log***

  The system log can give you important information about the functioning of your device and possible problems. You can adjust the scope of the system log to suit your needs (see the section entitled "System Log" on page 126).

➔ Click ***Refresh*** to refresh this screen and update the displayed data.

Installing the Printer Port for Network Printers

Your Gigaset SX541 WLAN dsl is equipped with a USB port that you can use, for example, to connect a printer for use as the network printer.

Introduction

A network printer is a printer on which you can print your documents without it being connected to your PC, for example to LPT1, the parallel interface. This has the advantage that you only need this printer once in your network. All PCs for which it is released can access it and work with it.

In most cases, a printer of this type is connected to another PC in the network. This does indeed offer the advantage referred to above, but it has serious disadvantages:

- The printer can only be used by others if the PC to which it is connected is switched on.
- The print job you send to the PC on which the printer depends reduces the performance (resources) of this PC.

If you use the USB port on the Gigaset SX541 WLAN dsl for your printer, you have all the advantages of a network printer without the disadvantages referred to above:

- The network, and consequently also the printer, is always ready (the Gigaset SX541 WLAN dsl and the printer itself must be switched on, of course).
- As it is connected to the USB printer port on your Gigaset SX541 WLAN dsl, it does not detract from the performance of any other PC in the network.

To facilitate this option, you must first set up a **printer port** on each PC wanting to use the network printer. A printer port is an interface on the PCs that forwards the print job to an IP address within the network.

Once you have set up this port, you must install the printer driver.

Note:

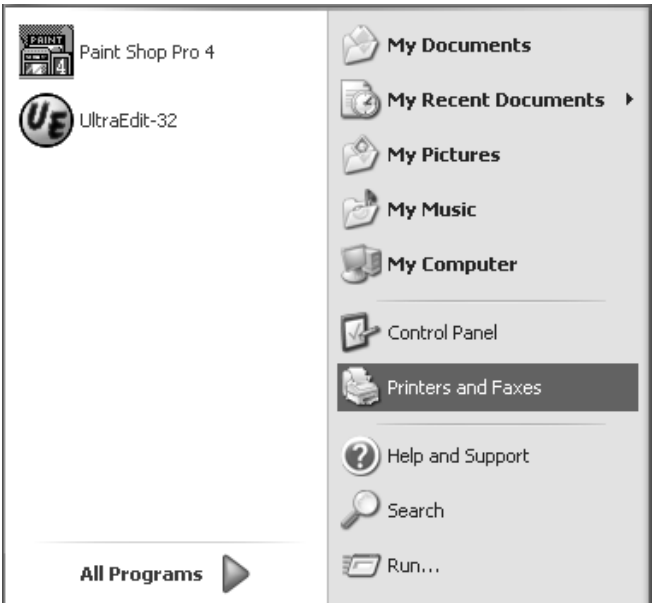
For multifunction devices (combination of printer, copier or fax) only the printer functionality is supported.

The printer server can only be used at present with selected printers that support USB V2.0. You can obtain further information by contacting the hotline or else on the Internet (see Quick Start Guide).

Installing a Standard TCP/IP Printer Port Under Windows XP/ 2000

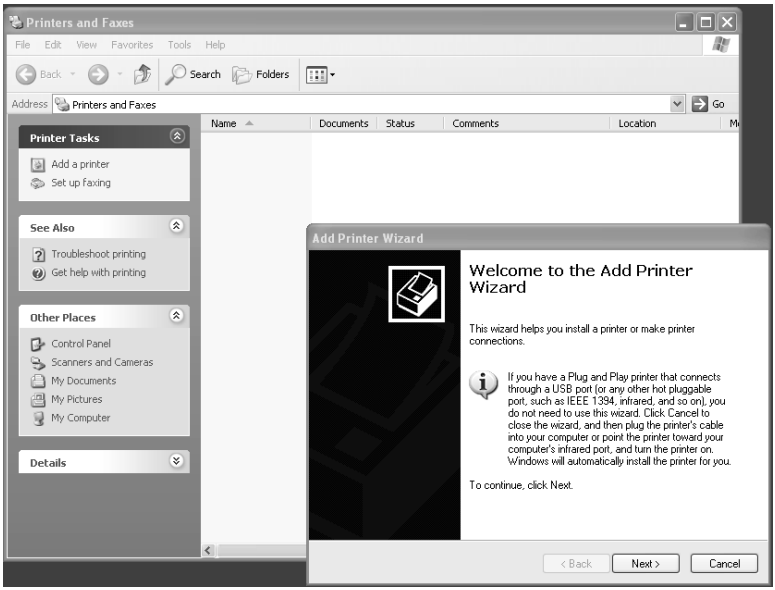
You can use the standard TCP/IP port driver present in this operating system. Make sure that the Gigaset SX541 WLAN dsl is connected and can be reached in the network. A printer need not be connected to the USB port on your Gigaset SX541 WLAN dsl at this point. The following illustrations show installation on Windows XP. Installation on Windows 2000 is essentially the same.

➞ Click ***Start*** and in the window that opens click ***Printer and Faxes***.

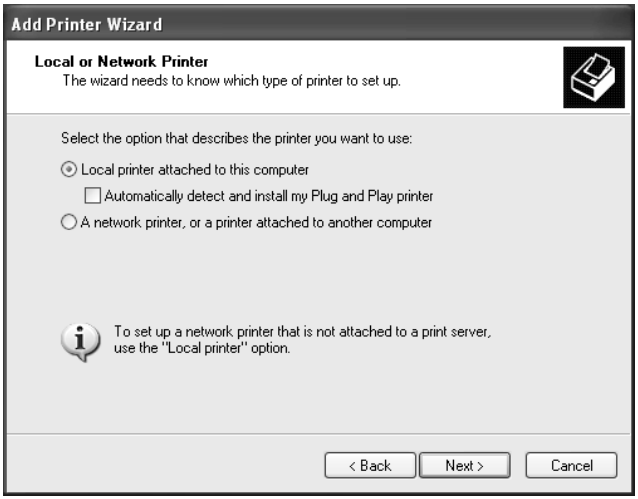


➞ Double click ***Add a printer*** in the window that opens.

The wizard for installing a printer is opened.


Printers and Faxes
File Edit View Favorites Tools Help
Back Search Folders
Address Printers and Faxes
Go
Printer Tasks
Add a printer
Set up faxing
See Also
Troubleshoot printing
Get help with printing
Other Places
Control Panel
Scanners and Cameras
My Documents
My Pictures
My Computer
Details
Name
Documents
Status
Comments
Location
Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

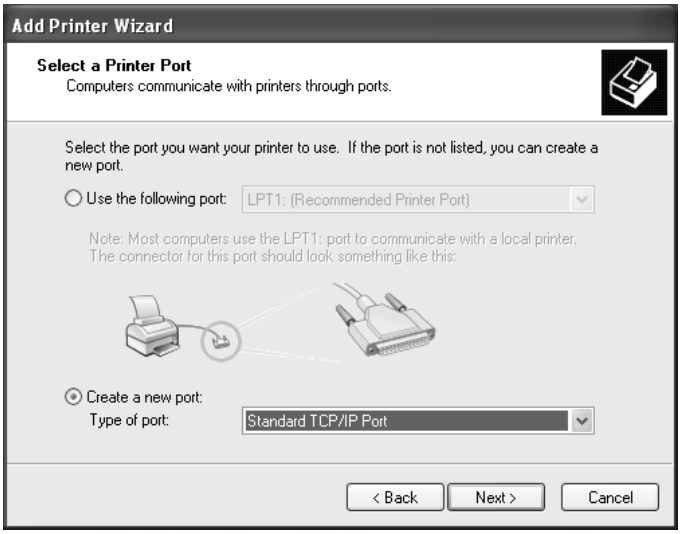
➔ In the printer wizard, click ***Next***.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

The printer port you are installing will behave like an additional parallel connection to the PC. For this reason, you must click the option button next to ***Local printer*** in this window.

The check box below should not be ticked in the square ***Plug & Play printer***. If there is a tick present, click the box to remove it.

➔ Click ***Next***.


Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Standard TCP/IP Port
< Back
Next >
Cancel

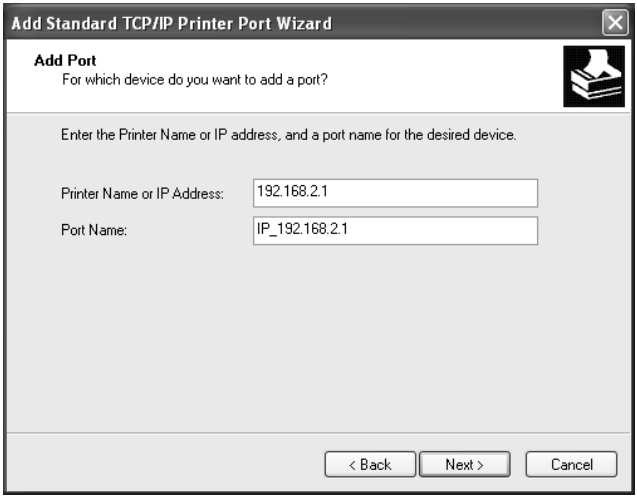
➔ Click the option button ***Create a new port***.

➔ Then select ***Standard TCP/IP Port*** from the selection menu in the field next to it.

➔ Click ***Next***.

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

➔ In the wizard for setting up a standard TCPI/IP port, click ***Next***.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.2.1
Port Name:
IP_192.168.2.1
< Back
Next >
Cancel

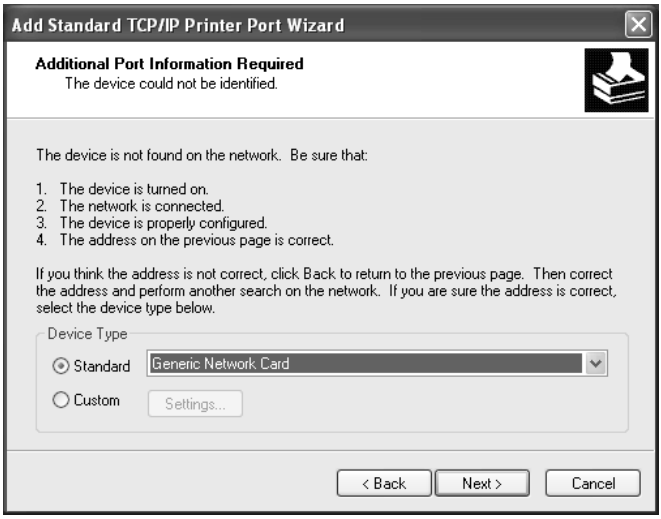
➔ In the ***Printer Name or IP Address*** input field, enter the IP address of the print server (Gigaset SX541 WLAN dsl): for example 192.168.2.1.

Your input is shown repeated in the second field.

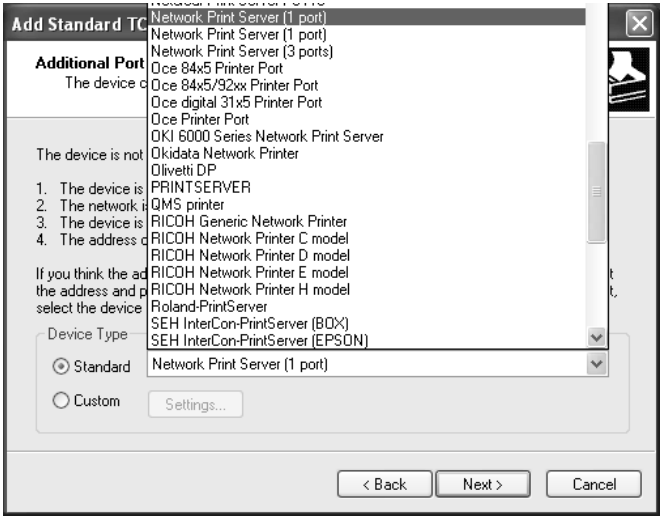
➔ Double click in the ***Port Name*** field and enter a name. This name will appear in the list of printer ports. Call this port, for example, **Gigaset_Printerport**.

➔ Click ***Next***.

As Windows XP usually first looks for a network card when a printer port is installed, the ***Additional Port Information Required*** window is shown.

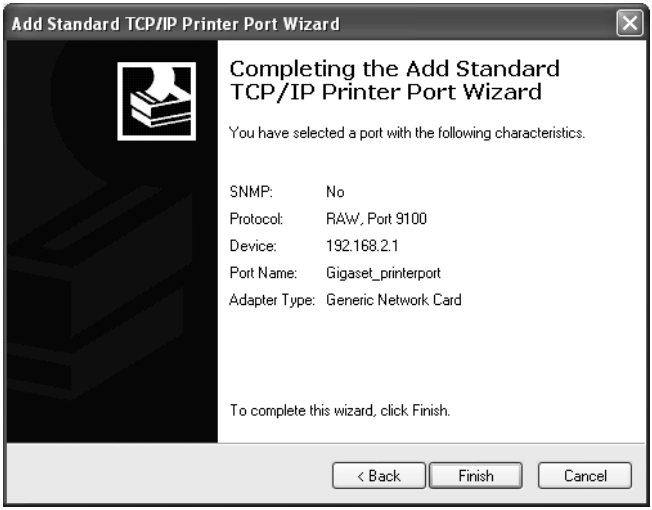

Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

➔ From the list of standard device types, select the offered type ***Network Print Server (1 port)*** (print server with a printer connection).



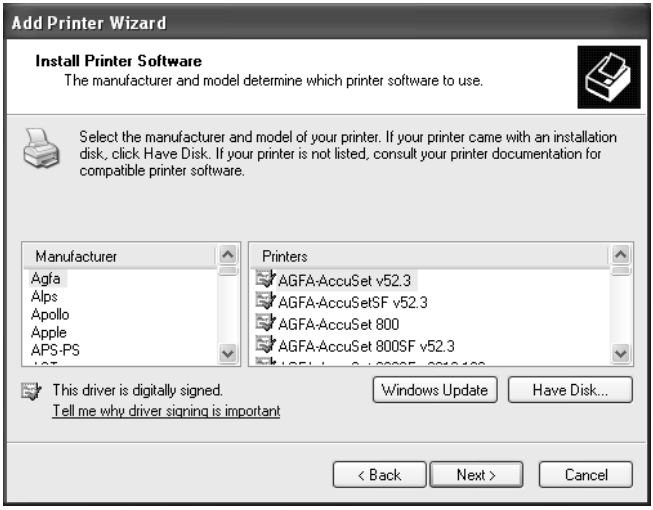
➔ Click ***Next***.

The window for finishing the wizard is opened and shows you all the settings you have made.


Add Standard TCP/IP Printer Port Wizard
Completing the Add Standard TCP/IP Printer Port Wizard
You have selected a port with the following characteristics.
SNMP: No
Protocol: RAW, Port 9100
Device: 192.168.2.1
Port Name: Gigaset_printerport
Adapter Type: Generic Network Card
To complete this wizard, click Finish.
< Back
Finish
Cancel

➔ Click ***Finish***.

Once the wizard for installing the printer port is finished, the ***Add Printer Wizard*** is opened.


Add Printer Wizard
Install Printer Software
The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Manufacturer
Agfa
Alps
Apollo
Apple
APS-PS
Printers
AGFA-AccuSet v52.3
AGFA-AccuSetSF v52.3
AGFA-AccuSet 800
AGFA-AccuSet 800SF v52.3
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
< Back
Next >
Cancel

➔ If you wish to install a printer for this port immediately, click ***Next*** and follow the printer installation wizard's instructions.

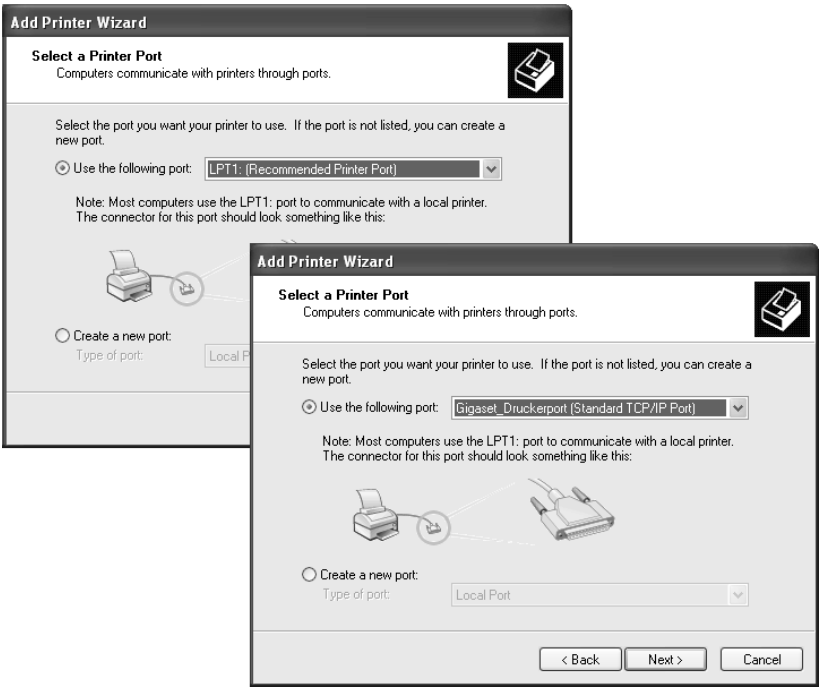
➔ If you do not wish to install a printer until later, click ***Cancel***.

Note:

The Gigaset SX541 WLAN dsl's printer server does not work bidirectionally. It does not evaluate any of the printer's response messages. For this reason please make sure that your printer is also configured unidirectionally. You can make the relevant printer settings for your printer via ***Start*** – ***Settings*** – ***Printer***.

Installing a Printer on the TCP/IP Port Retrospectively

If you connect a printer to this port at a later time, start as described above for installing the printer port.


Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
Gigaset_Druckerport (Standard TCP/IP Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Local Port
< Back
Next >
Cancel

➔ In this case, however, you should click the selection menu in the ***Select a Printer Port*** window.

➔ Select the connection you have set up from the list: for example ***Gigaset_printerport (Standard TCP/IP Port)***.

➔ Click ***Next*** and finish installing the printer driver as instructed in the windows that follow.

Installing a Printer Driver Under Windows 98 SE or ME

The following section describes how to install a printer driver under the Windows 98 SE or ME operating systems as the procedure and windows shown for these operating systems are very similar. The printer driver does not need to be installed on Windows XP and 2000.

You have installed your network and it is ready for use.

➔ Insert the CD-ROM included in the scope of delivery into the CD-ROM or DVD drive of your PC.

➔ Wait until the CD-ROM welcome window appears.

➔ Click Gigaset SX541 WLAN dsl.

➔ Click ***Printer port driver*** for Windows 98 SE or ME.

The welcome window for installing the port driver is opened.

➔ Read the information it contains carefully.

➔ Click ***Next***.

The necessary files are copied to your PC and executed. Once all the data has been transferred to your PC, you are prompted to complete the installation of the port driver.

➔ Click ***Finish***.

➔ Reboot your PC.

You have now installed the printer port and effectively installed an extra printer interface in your PC.

You must carry out this installation on every PC with Windows 98 or ME that is to use this printer in the network.

You might possibly still have to correct the IP address for the printer.

➔ Select ***Start*** – ***Settings*** – ***Printers***, select the printer and right-click the mouse to open the pop-up menu.

➔ Select ***Properties*** and open the ***Details*** tab.

➔ Select the port and click ***Port Settings***.

➔ Change the IP address if necessary. It must be the same as that for the Gigaset SX541 WLAN dsl.

Instructions for Setting up a Printer on the PC

Once you have installed the printer port you still cannot start printing. The printer port is nothing more than an additional interface on your PC, comparable with the USB port. It means that any printer you install on this port is also regarded as a local printer even though it is located in the network and possibly remote from you.

You still need to connect and configure the printer to this port.

➔ Connect the printer to the USB interface on your Gigaset SX541 WLAN dsl.

The printer is installed in the same way as any other printer:

➔ Go to ***Start*** – ***Settings*** – ***Printers*** and click ***Add Printer***.

➔ In the window that opens, click ***Next***.

➔ Proceed as instructed by the printer installation wizard. Please note:

In the window in which you are prompted to specify the location of the printer, you should select ***Local printer*** (usually the default setting).

➔ Then click ***Next***.

➔ Continue to install the printer. Select your printer and click ***Next***.

➔ When the window appears in which you are prompted to enter the type of connection, double click the port name ***Gigaset_printerport***.

➔ Then continue to install the printer and finish the installation.

Note:

The Gigaset SX541 WLAN dsl's printer server does not work bidirectionally. It does not evaluate any of the printer's response messages. For this reason please make sure that your printer is also configured unidirectionally.

Appendix

Troubleshooting

This chapter describes common problems and their solution. The Gigaset SX541 WLAN dsl is easy to monitor thanks to its LED displays. Problems can be quickly identified. If you cannot solve the connection problem after checking the LED displays, please consult the other sections of the following table.

Symptom	Possible cause and solutions
Power lamp does not light up.	No power supply. ➔ Check whether the mains adapter is connected to the Gigaset SX541 WLAN dsl and a power outlet. ➔ Check whether the device is switched on. ➔ Check whether the power outlet and the mains adapter are working properly. If the mains adapter is not working properly, please get in touch with our customer service unit (see Quick Start Guide).
The LAN LED on a connected device does not light up.	No LAN connection ➔ Make sure that the connected device is switched on. ➔ Check whether the Ethernet cable is plugged in. ➔ Check that you are using the right cable type (CAT5) and that the cable is not too long (100 m). ➔ Check that the network card on the connected device and the cables are not defective. If necessary, replace a defective network card or cable. ➔ Use the Windows device manager (***My Computer*** – ***Properties***) to check whether the network card is functioning. If you see a red cross or a question mark, then the driver may not have been installed or there is a resource conflict. Follow the Windows instructions to remedy the problem.
The ADSL LED does not light up after synchronisation.	➔ Check the cable. Check that the cable is correctly connected to the splitter.

Symptom	Possible cause and solutions
You cannot connect to the Internet.	➞ Check whether the ***Connect on demand*** option is deactivated. In this case, connections cannot be opened automatically. ➞ Select ***Connect on demand***. Remember that this setting may lead to higher costs if you are billed on the time used. ➞ The connection may have been terminated manually with the ***Connect on demand*** option selected. – Open the connection manually using the ***Connect*** button again or – restart the Gigaset SX541 WLAN dsl. In both cases, the ***Connect on demand*** setting will be active again. ➞ Check whether you have exceeded the ***Time and Volume Contingent*** for your Internet use.
You cannot open a connection from a wireless device to the Gigaset SX541 WLAN dsl.	The wireless network adapter is not using the correct SSID. ➞ Change the SSID on the network adapter. Either encryption is enabled on the Gigaset SX541 WLAN dsl but not on the wireless network adapter, or it is not using the correct key or is using another type of encryption. ➞ Activate the same encryption on the network adapter with the correct key. If you do not know the key, you will have to reset the Gigaset SX541 WLAN dsl (see page 18). **Warning**: Please bear in mind that this will restore **all** the configuration settings to the factory settings.

Symptom	Possible cause and solutions
The Gigaset SX541 WLAN dsl or other PCs cannot be reached by a PC in the connected LAN with a **ping** command.	➔ Make sure that TCP/IP has been installed and configured on all the PCs in the local network. ➔ Check that the IP addresses have been properly configured. In most cases you can use the Gigaset SX541 WLAN dsl's DHCP function to assign dynamic addresses to the PCs in the LAN. In this case, you have to configure the TCP/IP settings of all the PCs so that they obtain the IP address automatically. If you configure the IP addresses in the LAN manually, remember to use the subnet mask 255.255.255.x. This means that the first three parts of the IP address on each PC and the Gigaset SX541 WLAN dsl have to be identical. The device also has to be configured as a DNS server.
No connection to the Gigaset SX541 WLAN dsl's configuration environment.	➔ Use the **ping** command to check whether you can establish a network connection to the Gigaset SX541 WLAN dsl. ➔ Check the network cable between the PC you want to use to administer the device and the Gigaset SX541 WLAN dsl. ➔ If the PC you want to use is in the device's local network, make sure that you are using the correct IP address administration (see above). ➔ If the PC you want to use is not in the router's local network, it must be authorised via remote management.
Password forgotten or lost	➔ Reset the Gigaset SX541 WLAN dsl (see page 19). **Warning**: Please bear in mind that this will restore **all** the configuration settings to the factory settings.
You cannot access a resource (drive or printer) on a different PC.	➔ Make sure that TCP/IP has been installed and configured on all the PCs in the local network and that the PCs all belong to the same workgroup. ➔ Check whether the resource has been released on the PC in question and whether you have the necessary access rights. ➔ Printing: Check whether the printer has been set up as a network printer.

Specifications

Interfaces

1 DSL	RJ11, Annex A (U-R2)
4 LAN	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
1 USB	USB 1.1, for printer server or file server
1 FXO	RJ11, for connecting to the analogue subscriber line
2 FXS	RJ11, for connecting analogue end devices (telephone, fax, answerphone)
WLAN	802.11g, for the wireless connection of up to 252 PCs

Wireless properties

Frequency range	2,400 to 2,484 GHz ISM band
Spreading	Direct Sequence Spread Spectrum (DSSS)
Modulation	CCK, OFDM
Number of channels	IEEE 802.11b: 13 (Europe, ETSI) IEEE 802.11g: 13 (Europe, ETSI)
Transmission rate	IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

Operating environment

Temperature	Operating temperature 0 to 40 °C
	Storage temperature -10 to 70 °C
Humidity	5% to 80% (non condensing)
LED displays (green)	PWR ADSL (operation, synchroniastion) Online (activity, Internet) WLAN (activity, wireless) LAN1 to LAN4 (connection to PC, activity, wired) USB (device connection) VoIP (connection, activity, Internet telephony) Pone1 / Phone2 (FS activity) Line (FXO activity, fixed network)

Compliance with security conditions and regulations

CE, EN60950

Software	Browser-based configuration environment NAT, PPPoE, PPPoA DHCP server and client NAT, Port Forwarding, Port Triggering, Exposed Host Security Setup Firewall, prevention of hacker attacks MAC address filtering URL filtering, DoS blocking, SPI Log file WEP encryption WPA2 / WPA encryption SIP

Open Source Software used in the product

The product contains, among other things, embedded Open Source Software, licensed under an Open Source Software License and developed by third parties. These embedded Open Source Software files are protected by copyright. Your rights to use the Open Source Software beyond the mere execution of Siemens' program, is governed by the relevant Open Source Software license conditions.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between Siemens license conditions and the Open Source Software license conditions, the Open Source Software conditions shall prevail with respect to the Open Source Software portions of the software. The license conditions can be found at the following internet websites:

http://www.fsf.org/licensing/licenses/gpl.txt

http://www.fsf.org/licensing/licenses/lgpl.txt

If programs contained in this product are licensed under GNU General Public License (GPL) and/or GNU Lesser General Public License (LGPL) and this software is not already delivered in source code form together with the device, you can download the source code and the copyright notices of the relevant software from the internet at:

http://now-portal.c-lab.de/projects/gigaset

Additionally you can request the corresponding source code from SIEMENS by paying a fee 7.- € for the physical act of transferring the copy. Please send your specific request, together with a receipt indicating the date of purchase, within three years of your purchase, together with the ID number of the device and the software release number to:

Kleinteileversand Com Bocholt
E-Mail: kleinteileversand@bch.siemens.com
Fax: +49 2871 / 91 30 29

Warranty regarding further use of the Open Source Software:

SIEMENS provides no warranty for the Open Source Software programs contained in this device, if such programs are used in any manner other than the program execution intended by SIEMENS. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. SIEMENS specifically disclaims any warranties for defects caused by altering any Open Source Software program or the product's configuration. You have no warranty claims against SIEMENS in the event that the Open Source Software infringes the intellectual property rights of a third party.

Technical support, if any, will only be provided for unmodified software.

Open Source Software Licenses

GPL

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the

integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>
>
> Copyright (C) <year> <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) year name of author
>
> Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.
>
> This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program ‘Gnomovision’ (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989
>
> Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

LGPL

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria

of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to

this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the library's name and a brief idea of what it does.>
>
> Copyright (C) <year> <name of author>
>
> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the library 'Frob' (a library for tweaking knobs) written by James Random Hacker.
>
> <signature of Ty Coon>, 1 April 1990
>
> Ty Coon, President of Vice

That's all there is to it!

Glossary

Access Point

An Access Point, such as the Gigaset SX541 WLAN dsl, is the centre of a wireless local network (WLAN). It handles the connection of the wireless linked network components and regulates the data traffic in the wireless network. The Access Point also serves as an interface to other networks, for example an existing Ethernet LAN or via a modem to the Internet. The operating mode of wireless networks with an Access Point is called Infrastructure mode.

Ad-hoc mode

Ad-hoc mode describes wireless local networks (WLANs) in which the network components set up a spontaneous network without an Access Point for example several Notebooks in a conference. All the network components are peers. They must have a wireless Network adapter.

Auto Connect

Auto Connect means that applications such as Web browser, Messenger and Email automatically open an Internet connection when they are launched. This can lead to high charges if you are not using Flat rate. This function can be deactivated at the Gigaset SX541 WLAN dsl to save call charges.

Bridge

A Bridge connects several network segments to form a joint network, for example to make a TCP/IP network. The segments can have different physical characteristics, for example different connections such as Ethernet and wireless LANs. Linking individual segments via Bridges allows local networks of practically unlimited size.

See also: Switch, Hub, Router, Gateway

Broadcast

A Broadcast is a data packet not directed to a particular recipient but to all the network components in the network. The Gigaset SX541 WLAN dsl does not pass broadcast packets on; they always remain within the local network (LAN) it administers.

BSSID

Basic Service Set ID

BSSID permits unique differentiation of one wireless network (WLAN) from another. In Infrastructure mode, the BSSID is the MAC address of the Access Point. In wireless networks in Ad-hoc mode the BSSID is the MAC address of any one of the participants.

Client

A Client is an application that requests a service from a Server. For example, an http Client on a PC in a local network requests data, i.e. Web pages from an HTTP Server on the Internet. Frequently the network component (for example the PC) on which the Client application is running is also called a Client.

DHCP

Dynamic Host Configuration Protocol

DHCP handles the automatic assignment of IP addresses to network components. It was developed because in large networks – especially the Internet – the defining of IP addresses is very complex as participants frequently move, drop out or new ones join. A DHCP Server automatically assigns the connected network components (DHCP Clients) Dynamic IP addresses from a defined IP pool range thus saving a great deal of configuration work. In addition, the address blocks can be used more effectively: since not all participants are on the network at the same time, the same IP address can be assigned to different network components in succession as and when required.

The Gigaset SX541 WLAN dsl includes a DHCP server and uses it to assign automatic IP addresses to PCs in the local network. You can specify that the IP addresses for certain PCs are never changed.

DHCP Server

See DHCP

DMZ

Demilitarised Zone

DMZ describes a part of a network that is outside the Firewall. A DMZ is set up, as it were, between a network you want to protect (for example a LAN) and an insecure network (for example the Internet). A DMZ is useful if you want to offer Server services on the Internet which for security reasons are not to be run from behind the firewall or if Internet applications do not work properly behind a firewall. A DMZ permits unrestricted access from the Internet to only one or a few network components, while the other network components remain secure behind the firewall.

DNS

Domain Name System

The assignment of DNS permits IP addresses to computers or Domain names that are easier to remember. A DNS server must administer this information for each LAN with an Internet connection. As soon as a page on the Internet is called up, the browser obtains the corresponding IP address from the DNS Server so that it can establish the connection.

The assignment of domain names to IP addresses on the Internet follows a hierarchical system. A local PC only knows the address of the local Name Server. This in turn knows all the addresses of the PCs in the local network and the superordinated Name Servers, which again know addresses and the next superordinated Name Servers.

DNS server

See DNS

Domain name

The Domain name is the reference to one or more Web servers on the Internet.
The Domain name is mapped via the DNS service to the corresponding IP address.

DoS attack

Denial of Service

A DoS attack is a particular form of hacker attack directed at computers and networks with a connection to the Internet. The aim is not so much to steal data but to paralyse the computer or network so severely that the network resources are no longer available. A typical hacker attack involves making a remote computer announce that it is acting for the paralysed computer, for example, and receive the data meant for you.

DSL

Digital Subscriber Line

DSL is a data transmission technique in which a connection to the Internet can be run at 1.5 Mbps over normal telephone lines. A DSL connection is provided by an Internet Provider. It requires a DSL modem.

Dynamic IP address

A dynamic IP address is assigned to a network component automatically by the DHCP. This means that the IP address of a network component can change with every login or at certain intervals.

See also Static IP address

DynDNS

Dynamic DNS

The assignment of Domain names and IP addresses is handled by the Domain Name Service (DNS). For Dynamic IP addresses this service is now enhanced with so-called Dynamic DNS (DynDNS). It enables the use of a network component with a dynamic IP address as a Server on the Internet. DynDNS ensures that a service can always be addressed on the Internet under the same Domain name regardless of the current IP address.

Encryption

Encryption protects confidential information against unauthorised access. With an encryption system, data packets can be sent securely over a network. The Gigaset SX541 WLAN dsl offers WEP encryption and WPA for secure data transmission over wireless networks.

Ethernet

Ethernet is a network technology for local networks (LANs) defined by the IEEE as standard IEEE 802.3. Ethernet uses a base band cable with a transmission rate of 10 or 100 Mbps.

Exposed Host

Exposed Host refers to a PC outside the firewall.

See also DMZ

Firewall

Firewalls are used by network operators as protection against unauthorised external access. This involves a whole bundle of hardware and software actions and technologies that monitor and control the data flow between the private network to be protected and an unprotected network such as the Internet.

See also NAT

Flat rate

Flat rate is a particular billing system for Internet connections. The Internet Provider charges a monthly fee regardless of the duration and number of logins.

Full duplex

Data transmission mode in which data can be sent and received at the same time.

See also Half duplex

Gateway

A gateway is a device for connecting networks with completely different architectures (addressing, protocols, application interfaces etc.). Although it is not totally correct, the term is also used as a synonym for Router.

Global IP address

See Public IP address

Half duplex

Operating mode for data transfer. Only one party can receive or send data at a time.

See also Full duplex

HTTP Proxy

An HTTP proxy is a Server that network components use for their Internet traffic. All requests are sent via the proxy.

Hub

A Hub connects several network components in a star-topology network by sending all the data it receives from one network component to all the other network components.

See also: Switch, Bridge, Router, Gateway

IEEE

Institute of Electrical and Electronic Engineers

The IEEE is an international body for defining network standards, especially for standardising LAN technologies, transmission protocols and speeds and wiring.

IEEE 802.11

IEEE 802.11 is a standard for wireless LANs operating in the 2.4 GHz band. In so-called Infrastructure mode, terminals can be connected to a base station (Access Point) or they can connect with each other spontaneously (Ad-hoc mode).

IGMP

Internet Group Management Protocol

IGMP is an Internet Protocol that enables an Internet computer to inform neighbouring routers that it is a member of a multicast group. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the first computer's content. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.

Infrastructure mode

Infrastructure mode is a way of operating wireless local networks (WLANs) in which an Access Point handles the data traffic. Network components cannot establish a direct connection with each other as is the case in Ad-hoc mode.

Internet

The Internet is a wide-area network (WAN) linking several million users around the world. A number of Protocols have been created for exchanging data, and these are known collectively as TCP/IP. All participants on the Internet are identifiable by an IP address. Servers are addressed by a Domain names (for example siemens.com). Domain names are assigned to IP addresses by the Domain Name Service (DNS).

Among the most important Internet services are:

- electronic mail (email)
- the World Wide Web (WWW)
- file transfer (FTP)
- discussion forums (Usenet / Newsgroups)

Internet Provider

An Internet Service Provider offers access to the Internet for a fee.

Internet telephony

Voice transmission via the Internet (Voice over IP).

IP

Internet Protocol

The IP Protocol is one of the TCP/IP protocols. It is responsible for addressing parties in a network using IP addresses, and routes data from the sender to the recipient. It decides the paths along which the data packets travel from the sender to the recipient in a complex network (routing).

IP address

The IP address is the unique network-wide address of a network component in a network based on the TCP/IP protocol (for example in a local network (LAN) or on the Internet). The IP address has four parts (decimal numbers) separated by full stops (for example 192.168.1.1). The IP address comprises the network number and the computer number. Depending on the Subnet mask, one, two or three parts form the network number, the remainder forms the computer number. You can find out the IP address of your PC using the **`ipconfig`** command.

IP addresses can be assigned manually (see Static IP address) or automatically (see Dynamic IP address).

On the Internet, Domain names are normally used instead of the IP addresses. DNS is used to assign domain names to IP addresses.

The Gigaset SX541 WLAN dsl has a Private IP address and a Public IP address.

IP pool range

The Gigaset SX541 WLAN dsl's IP address pool defines a range of IP addresses that the router's DHCP Server can use to assign Dynamic IP addresses.

ISP

(Internet Service Provider)

Internet Provider

LAN

Local network

A local network links network components so that they can exchange data and share resources. The physical range is restricted to a particular area (a site). As a rule, the users and operators are identical. A local network can be connected to other local networks or to a wide-area network (WAN) such as the Internet.

With the Gigaset SX541 WLAN dsl, you can set up a wired local Ethernet network and a wireless IEEE 802.11g standard network (WLAN).

Lease time

The lease time defines the period of time for which the PCs keep the Dynamic IP address assigned to them by the DHCP server without changing them.

Local IP address

See Private IP address

MAC address

Media Access Control

The MAC address is used for the globally unique identification of a Network adapter. It comprises six parts (hexadecimal numbers), for example 00-90-96-34-00-1A. The MAC address is assigned by the network adapter manufacturer and cannot be changed.

Mbps

Million bits per second

Specification of the transmission speed in a network.

MER

MAC Encapsulated Routing

MRU

Maximum Receive Unit

The MRU defines the maximum user data volume within a data packet.

MTU

Maximum Transmission Unit

The MTU defines the maximum length of a data packet that can carried over the network at a time.

NAT

Network Address Translation

NAT is a method for converting IP addresses (mostly Private IP addresses) within a network into one or several Public IP addresses on the Internet. With NAT, several network components in a LAN can share the router's public IP address to connect to the Internet. The network components of the local network are hidden behind the router's IP address registered on the Internet. Because of this security function, NAT is frequently used as part of the Firewall of a network. If you want to make services on a PC in the local network available on the Internet despite NAT, you can configure the Gigaset SX541 WLAN dsl as a Virtual server.

Network

A network is a group of devices connected in wired or wireless mode so that they can share resources such as data and peripherals. A general distinction is made between local area networks (LANs) and wide area networks (WANs).

Network adapter

The network adapter is the hardware device that creates the connection between a network component and a local network. The connection can be wired or wireless. An Ethernet network card is an example of a wired network adapter. The Gigaset PC Card and the Gigaset USB Adapter are examples of wireless network adapters.

A network adapter has a unique address, the MAC address.

Port

Data is exchanged between two applications in a network across a port.The port number addresses an application within a network component. The combination of IP address/port number uniquely identifies the recipient or sender of a data packet within a network. Some applications (for example Internet services such as HTTP or FTP) work with fixed port numbers, others are allocated a free port number whenever they need one.

Port Forwarding

In port forwarding the Gigaset SX541 WLAN dsl directs data packets from the Internet that are addressed to a particular Port to the corresponding port of the appropriate network component. This enables servers within the local area network to offer services on the Internet without them needing a Public IP address.

See also: Virtual server

PPPoA

Point-to-Point Protocol over ATM

PPPoA is a Protocol for connecting network components in a local Ethernet network to the Internet via an ATM network.

PPPoE

Point-to-Point Protocol over Ethernet

PPPoE is a Protocol for connecting network components in a local Ethernet network to the Internet via a modem.

Private IP address

The private IP address (also known as the local IP address) is a network component's address within the local area network (LAN). The network operator can assign any address he or she wants. Devices that act as a link from a local network, such as the Gigaset SX541 WLAN dsl, have a private and a Public IP address.

Protocol

A protocol describes the agreements for communicating in a network. It contains rules for opening, administering and closing a connection, as well as about data formats, time frames and handling possible errors. Communications between two applications require different protocols at various levels, for example the TCP/IP protocols for the Internet.

Public IP address

The public IP address (also known as the global IP address) is a network component's address on the Internet. It is assigned by the Internet Provider. Devices that create a link from a LAN to the Internet, such as the Gigaset SX541 WLAN dsl, have a public and a Private IP address.

Radio network

See WLAN

Rekey Interval

The rekey interval is the period after which new keys are automatically generated for data encryption with WPA-PSK.

Remote Management

Remote Management refers to the ability to manage a network from a network component that is actually outside the local area network (LAN).

Repeater

A repeater extends the range of a wireless local area network by relaying data from the Access Point to additional PCs or Network adapters.

Roaming

Roaming extends the range of a wireless LAN by using several Access Points that use the same SSID and the same radio channel and are linked via Ethernet. The PCs in the network can switch dynamically between several Access Points without losing the existing network connection.

Router

A router directs data packets from one local area network (LAN) to another via the fastest route. A router makes it possible to connect networks that have different network technologies. For example, it can link a local network with Ethernet or WLAN technology to the Internet.

See also: Bridge, Switch, Hub, Gateway

Server

A server makes a service available to other network components (Clients). The term "server" is often used to refer to a computer or PC. However it can also mean an application that provides a particular service such as DNS or a Web service.

SIP

Session Initiation Protocol

SIP is a standard for data transfer in Internet telephony (VoIP). It describes how a call is carried over the data network and which components plus which transport and signalling protocols are involved.

SMTP

Simple Mail Transfer Protocol

The SMTP Protocol is part of the TCP/IP protocol family. It governs the exchange of electronic mail on the Internet. Your Internet Provider provides you with access to an SMTP server.

SNMP

Simple Network Management Protocol

The SNMP Protocol is part of the TCP/IP protocol family. It provides a simple procedure for administering the network based on a system of shared information for management data and network management messages (known as traps) and reports the occurrence of events within the monitored network (for example an alarm message or notification of configuration changes).

SSID

Service Set Identifier

The SSID is used to identify the stations in a wireless network (WLAN). All wireless network components with the same SSID form a common network. The SSID can be assigned by the network operator.

Static IP address

A static IP address is assigned to a network component manually during network configuration. Unlike a Dynamic IP address, a static (fixed) IP address never changes.

Subnet

A subnet divides a network into smaller units.

Subnet mask

The subnet mask determines how parts of the IP addresses of a network represent the network number and how many the computer number.

The subnet mask in a network administered by the Gigaset SX541 WLAN dsl is always 255.255.255.0. That means the first three parts of the IP address form the network number and the final part is used for assigning computer numbers. The first three parts of the IP address of all network components are in this case always the same.

Switch

A switch, like a Hub, is an element used to link different network segments or components. Unlike a Hub however, the Switch has its own intelligence that enables it to forward packets to only the subnet or network component they are meant for.

See also: Bridge, Hub, Router, Gateway

TCP

Transmission Control Protocol

The TCP Protocol is part of the TCP/IP protocol family. TCP handles data transport between communication partners (applications). TCP is a session-based transmission protocol, i.e. it sets up, monitors and terminates a connection for transporting data.

See also UDP

TCP/IP

Protocol family on which the Internet is based. IP forms the basis for every computer-to-computer connection. TCP provides applications with a reliable transmission link in the form of a continuous data stream. TCP/IP is the basis on which services such as WWW, Mail and News are built. There are other protocols as well.

UDP

User Datagram Protocol

UDP is a Protocol of the TCP/IP protocol family that handles data transport between communication partners (applications). Unlike TCP, UDP is a non-session based protocol. It does not establish a fixed connection. The data packets, so-called datagrams, are sent as a Broadcast. The recipient is responsible for making sure the data is received. The sender is not notified about whether it is received or not.

UPnP

Universal Plug and Play

UPnP technology is used for the spontaneous linking of home or small office networks. Devices that support UPnP carry out their network configuration automatically once they are connected to a network. They also provide their own services or use services of other devices in the network automatically.

URL

Universal Resource Locator

Globally unique address of a Domain on the Internet.

Virtual server

A virtual Server provides a service on the Internet, that runs not on itself, but on another network component. The Gigaset SX541 WLAN dsl can be configured as a virtual server. It will then direct incoming calls for a service via Port Forwarding directly to the appropriate Port of the network component in question.

VoIP

Voice over IP

See Internet telephony

WAN

Wide Area Network

A WAN is a network that is not restricted to one particular area, such as the Internet. A WAN is run by one or more public providers to enable private access. You access the Internet via an Internet Provider.

WEP

Wired Equivalent Privacy

WEP is a security protocol defined in the IEEE 802.11 standard. It is used to protect wireless transmissions in a WLAN against unauthorised access through Encryption of the data transmitted.

WLAN

Wireless LAN

Wireless LANs enable network components to communicate with a network using radio waves as the transport medium. A wireless LAN can be connected as an extension to a wired LAN or it can form the basis for a new network.The basic element of a wireless network is the cell. This is the area where the wireless communication takes place. A WLAN can be operated in Ad-hoc mode or Infrastructure mode.

WLAN is currently specified in Standard IEEE 802.11. The Gigaset SX541 WLAN dsl complies with Standard 802.11g.

WPA

WPA was developed to improve the security provided by WEP. WPA uses complex procedures to generate keys, such as TKIP (Temporal Key Integrity Protocol). In addition, WPA can use an authentication server (for example a RADIUS server) to increase security.

WPA-PSK

WPA Pre-shared Key

Variant of WPA data encryption, in which new keys are automatically generated at regular intervals by means of a keyword (Pre-shared Key). The key is updated after defined periods (Rekey Interval).

Index

Numerics

10/100 Mbps Switch Port 19
128-bit encryption 101
128-bit key 64, 100, 102
64-bit key 64, 100, 102

A

Access control 66, 81, 102
  blocking services 82
  local network 102
  schedule rule 84
Access Point 9, 95, 167
Access protection
  for data carrier 114
Access rules
  URL filter 83
Address block for
    IP addresses 93
Ad-hoc mode 9, 167
ADSL connection
  socket 19
Advanced settings
  features 68
Advanced Setup 50
Antenna 19
Anti-DoS firewall 78
ASCII key 65, 101
Attack detection 78
Authentication server 99
Auto Connect 167

B

Back panel 19
Backup 123
Base station see Access Point
Basic settings 50
  configuration 53
  summary 58
Bridge 167
Broadcast 96, 167
Browser 48
BSSID 167

C

Call waiting 107
Checking network settings
    (Windows XP) 24
Client 167
  for Microsoft network 38
CLIR 108
Command
  exit 37
  ipconfig /release 37
  ipconfig /renew 37
  ping 47
Command prompt
  opening 47
Configuration
  resetting to factory setting 124
  restoring 124
  security 59
Configuration data
  backing up 123
Configuration file 123
Configuration program
  idle time 121
Connect on demand 56, 72
Connection
  checking to router 47
  statistics 47
Connection duration 56
Connection method 23
Connection mode 56, 71
Creating a network installation
    disk (Windows XP) 24

D

Data carrier
  access protection 114
Data encryption 100
Deactivating HTTP proxy
  Windows 2000 36
  Windows 98 45
  Windows XP 28

Defining computer name
Windows 2000 31
Windows 98 39
Windows XP 24
Defining workgroup
Windows 2000 31
Windows 98 39
Windows XP 24
De-registering 52
DHCP 21, 168
DHCP server 94, 168
DHCP service see DHCP
Dialing plans 108
Digital Subscriber Line see DSL
DMZ 14, 89, 168
DNS 168
DNS configuration
Windows 2000 35
Windows 98 43
Windows XP 27
DNS Server 168
DNS server
defining 74
Domain name 168
Domain Name Service see DNS
DoS attack 78, 169
DSL 169
DSL interface
configuring 53
Dynamic DNS see DynDNS
Dynamic Host Configuration Protocol
see DHCP
Dynamic IP address 21, 169
DynDNS 90, 169
DynDNS service see DynDNS
DynDNS.org 90

E

Encryption 62, 97, 100, 102, 169
WEP 64
WPA 63
Ethernet 8, 9, 13, 169
transmission speed 13
Ethernet network
connecting to a wireless
network 11
Ethernet network architecture 8
Exit command 37
Exposed Host 14, 89

F

Features 13
File server 112
partition list 113
sharing directories 113
Firewall 14, 170
activating/deactivating 78
attack detection 78
configuring 78
e-mail notification 80
security level 79
user-defined 80
Flat rate 170
Front panel 17
Full duplex 170

G

Games on the Internet 86
Gateway 42, 170
Gigaset SE551 WLAN dsl
back panel 19
ways to set up the network 7
Gigaset SX 541 WLAN dsl
configuring 48
front panel 17
installation 15
IP address 48
protecting with password 60
setting up 19
Gigaset SX541 WLAN dsl
reset 19
Global IP address see
Public IP address

H

Hacker attack 14, 169
e-mail notification 80
Half duplex 170
Help 52
Hexadecimal 65, 101
Hexadecimal key 101
Hook flash time 108
HTTP proxy 170
Hub 170

I
Idle time 121
IEEE 170
Infrastructure mode 9, 171
Installation 15
Installing network services
(Windows 2000) 30
Installing printer driver
Windows 98, 2000 147
Windows XP 146
Installing TCP/IP protocol
Windows 2000 32
Windows 98 40
Institute of Electrical and Electronic Engineers see IEEE
Internet 171, 172
connect on demand 72
connection mode 56, 71
manual connection 72
menu 69
service provider 71
setting up access control 81
testing settings 72
Internet access 6
Internet connection
changing the configuration 70
closing manually 118
disconnecting automatically . . . 56, 72
opening manually 118
setting up 70
Internet Explorer 16, 48
Internet protocol see IP protocol
Internet provider 71, 171
Internet telephony 6, 12
analogue telephone 104
call waiting 107
dialing plans 108
quick dial 110
setting up 104
VoiP settings 105
Internet time 120
Internet use
limits 76
time limit 77
volume limit 77
IP address 93, 172
address block 93
assigning automatically 21, 93
assigning static 21, 94
dynamic 21, 169
Gigaset SX 541 WLAN dsl 48
private 174
public 174
static 176
IP address block for DHCP 94
IP address pool 172
IP protocol 171
ipconfig /release 37
ipconfig /renew 37
ISP see Internet provider

K
Key length 64
128 bit (ASCII) 65, 101
128 bit (hexadecimal) 65, 101
64 bit (ASCII) 65, 101
64 bit (hexadecimal) 65, 101
Key type 65

L
LAN 11, 172
LAN socket 19
Lease time 94, 172
LED
behaviour after initial connection . . 20
LED displays 17
Local IP address see Private IP address
Local network 6, 13, 172
configuring 21
Login screen 48

M
MAC access control list 66, 102
MAC address 172
changing registration 75
cloning 75
MAC address filter 66
MAC Encapsulated Routing see MER
MAC table 66
Mains adapter
socket 19
Manual connection 72

Maximum Receive Unit see MRU
Maximum Transmission Unit
see MTU
Mbps 173
MER 173
Mozilla Firefox 16, 48
MRU 173
MTU 173

N
NAT 85, 173
port forwarding 85
port triggering 85
Network 173
ad-hoc mode 9
infrastructure 9
wired 8
wireless 9
Network adapter 173
Ethernet 8
wireless 9
Network Address Translation 85
Network Address Translation see NAT
Network configuration 21
Windows 2000 30
Windows 98 38
Windows XP 21
Network printer 139

O
Obtaining an IP address automatically
Windows 2000 35
Windows 98 42
Windows XP 27
Opera 48
Operating state 17

P
Passphrase 65
Password 48, 60
assigning 60
changing 60
forgotten 60
PC
defining name
(Windows 2000) 31
defining name (Windows 98) 39
defining name (Windows XP) 24
IP address 21
network settings 21
setting up as client for Microsoft
networks 38
Ping command 47
Point-to-Point Protocol over ATM
see PPPoA
Point-to-Point Protocol over Ethernet
see PPPoE
Port 174
public port 85, 87
trigger port 85, 87
Port forwarding 85, 174
setting up 88
Port number 88, 174
illustration 88
Port triggering 85, 86
setting up 87
PPPoE 13, 174
PPPoE Pass-Through 56, 72
Pre-shared Key
Printer
connecting 148
installing on TCP/IP port 146
Printer interface
configuring 139
Printer port (TCP/IP)
installing 140
Printer server 117
Printer wizard 141
Private IP address 174
Problem solving 149
Protocol 174
Public IP address 174

Q
QoS (Quality of Service) 92
Quick dial 110
Quick dial numbers 110

R
Radio network 178
ad-hoc mode 9
infrastructure mode 9
RADIUS server 99
Reboot 124

Reboot function 19
Regional settings 119
Rekeying 63, 98
Releasing TCP/IP settings
Windows 2000 37
Windows 98 46
Windows XP 29
Remote management 121, 175
Removing hardware safely 111
Repeater 103
Reset 19, 124
Reset function 19
Roaming 175
Router 175
dynamic IP address 90
IP address 93
setting up local network 7

S

Safety precautions 5
Schedule rule 84
Security architecture, WEP 100
Security measures 14
Security settings 50, 59
saving 67
Server 175
virtual 177
Service Set Identifier see SSID
Session Initiation Protocol see SIP
Setting up a network client
(Windows 98) 39
Simple Mail Transfer Protocol see SMTP
Simple Network Management Protocol
see SNMP
SIP 175
SMTP 175
SNMP 176
Socket
for DSL connetcion 19
for mains adapter 19
LAN 19
USB 19
SPI 81
SPI (Stateful Packet Inspection) see SPI
SSID 15, 61, 176
changing 61
default setting on router 15
hidden 96
visible 61, 96
SSID broadcast 61, 96
Start screen 49
Stateful Packet Inspection 81
Static IP address 176
Status
device 137
local network 134
overview 127
security 129
telephony 136
time and volume control 133
wireless network 135
Status information 127
Subnet 176
Subnet mask 176
Switch 176
switch off 19
switch on 19
Synchronising the TCP/IP settings
with the router
Windows 2000 37
Windows 98 46
Windows XP 29
System log 126
System password
assigning 120
changing 120
System requirements 16
System time 120

T

TCP 176
TCP/IP 177
TCP/IP network 21
TCP/IP port for printer 146
TCP/IP settings
Windows 2000 34
Windows 98 41
Windows XP 25
Telephone
analogue 104
Telephone socket 19
splitter 19

Telephony
basic settings 57
hide own number. 108
hook flash time 108
VoiP account 57
Temperature range for operation 19
Time and volume control. 76
Time limit 77
Time server 120
TKIP (Temporal Key Integrity Protocol) 178
Trademarks 5
Transmission Control Protocol see TCP
Transmission mode 96
Transmission speed 173
in Ethernet LAN 13
in wireless LAN. 13
Trigger port 85

U
UDP. 177
UI elements 52
Universal Plug and Play see UPnP
Universal Resource Locator see URL
Updating firmware 125
Upgrading firmware 125
UPnP 56, 73, 177
activating 73
URL 177
URL filter 82
USB 111
file server 112
printer server 117
Web server 115
USB data carrier 111
USB port 111
USB socket. 19
User Datagram Protocol see UDP
User interface
buttons 52
launching 48

V
Vanity 110
VCI 169
Virtual server 14, 86, 177
Voice over IP see Internet telephony
Voip account 57
VoIP see Internet telphony
Volume limit 77
VPI 177

W
WAN 177
WAN interface 10
WDS. 103
Web server 115
FTP 116
HTTP service 116
WEP 62, 64, 97, 100, 178
encryption mode 100
hexadecimal 65
key length. 64, 101
passphrase 65
Wide Area Network see WAN
Wired Equivalent Privacy see WEP
Wired network 8
Wireless cell 178
Wireless LAN see WLAN
Wireless network
access control 66
encryption 62
Wireless settings 95
WLAN. 9, 11, 178
operating modes 9
transmission speed 13
WLAN adapter 9
WPA 63, 97, 178
Pre-shared Key
WPA2-PSK 62, 98
WPA-PSK 63, 98
WPA-PSK see WPA, Pre-shared Key

Issued by
Siemens Communications
Haidenauplatz 1
D-81667 Munich

© Siemens AG 2005
All rights reserved. Subject to availability.
Rights of modification reserved.

Siemens Aktiengesellschaft
www.siemens.com/gigaset

No.: A31008-M1025-L101-1-7619